FortiAuthenticator - VM Install Guide

VERSION 4.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

3/20/2017

FortiAuthenticator 4.3 - VM Install Guide

Revision 1

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-03-20	Added FortiAuthenticator KVM deployment, as support was introduced for FortiAuthenticator 4.3.
2017-03-07	Initial release for FortiAuthenticator 4.3.

Introduction

Welcome, and thank you for selecting Fortinet products to protect your network.

FortiAuthenticator VM is a virtual appliance designed specifically to provide authentication services for multiple devices, including firewalls, SSL and IPsec VPNs, wireless access points, switches, routers, and servers. FortiAuthenticator includes a RADIUS and LDAP server. Authentication servers are an important part of an enterprise network, controlling access to protected network assets, and tracking users' activities to comply with security policies.

FortiAuthenticator is not a firewall; it requires a FortiGate appliance to provide firewall-related services. Multiple FortiGate units can use a single FortiAuthenticator appliance for Fortinet Single Sign On (FSSO) and other types of remote authentication, two-factor authentication, and FortiToken device management. This centralizes authentication and FortiToken maintenance.

FortiAuthenticator provides an easy-to-configure remote authentication option for FortiGate users. Additionally, it can replace the FSSO Agent on a Windows AD network.

Whilst FortiAuthenticator is a hardened server it should be installed with adequate protection from the Internet. Management protocols should be configured on private networks and only the resources required exposed to the outside.

The FortiAuthenticator VM delivers centralized, secure two-factor authentication for a virtual environment with a stackable user license for the greatest flexibility. Supporting from 100 to 1 million+ users, the FortiAuthenticator VM supports the widest range of deployments, from small enterprise right through to the largest service provider.

Failure to protect the FortiAuthenticator may result in compromised authentication databases.

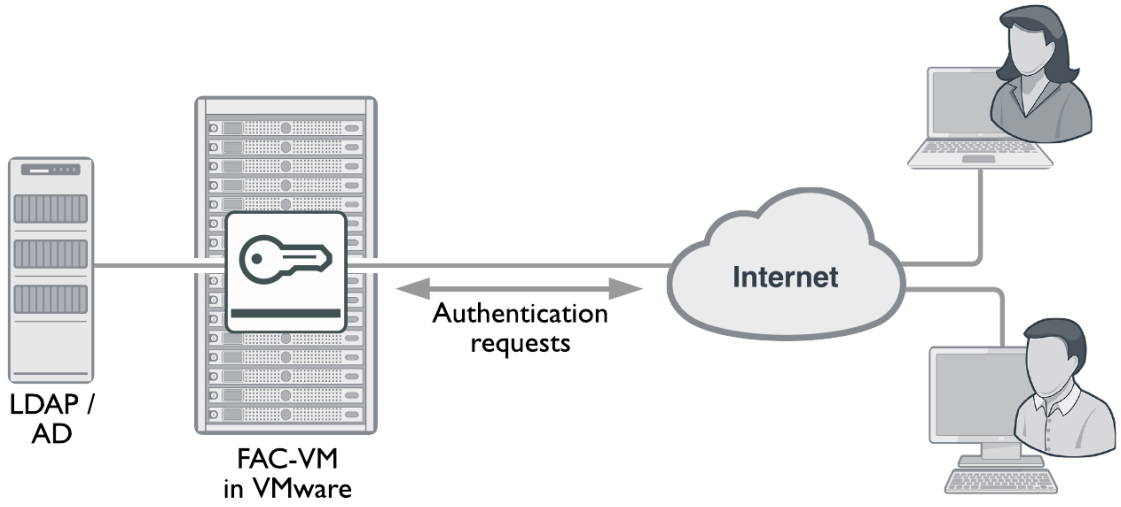
This document includes an overview of the FortiAuthenticator VM, its deployment with both VMware vSphere and MS Hyper-V clients, and information on how to perform an initial configuration.

Architecture

FortiAuthenticator VM is a virtual appliance version of FortiAuthenticator. It is deployed in a virtual machine environment such as VMware ESX (or ESXi), MS Hyper-V, or the Linux based Virtual Machine Manager.

Once the virtual appliance is deployed and set up, you can manage FortiAuthenticator VM via its Web-based Manager in a web browser on your management computer.

Figure 1: FortiAuthenticator VM architecture



FortiAuthenticator VM requires the following connectivity for management. Inbound management using Telnet and HTTP is not recommended. SSH is intended for initial configuration and diagnostics only. For more information, see the FortiAuthenticator Administration Guide.

Inbound management:

Service	Port
Telnet	TCP 23
HTTP	TCP 80
HTTPS	TCP 443
SSH	TCP 22

Outbound management:

Service	Port
DNSlookup	UDP 53
NTP	UDP 123
FortiGuard Licensing	TCP 443 (required for initial token registration)
Log Export (FTP)	TCP 21

FortiAuthenticator VM Overview

This section provides an overview of FortiAuthenticator VM.

The following topics are included in this section:

Licensing

Fortinet offers the FortiAuthenticator VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. When configuring your FortiAuthenticator VM, make sure to configure hardware settings as outlined in Table 3 and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

FortiAuthenticator VM license options:

SKU	Description
FAC-VM-Base	Base FortiAuthenticator-VM with 100 user licenses. Unlimited vCPU.
FAC-VM-100-UG	FortiAuthenticator-VM with 100 user license upgrade.
FAC-VM-1000-UG	FortiAuthenticator-VM with 1,000 user license upgrade.
FAC-VM-10000-UG	FortiAuthenticator-VM with 10,000 user license upgrade.
FAC-VM-100000-UG	FortiAuthenticator-VM with 100,000 user license upgrade.

Note that the FAC-VM-Base license is always required and that other licenses are upgrades to the base license.

Hypervisors supported:

- VMware ESXi 4.0/4.1/5.0/5.1/5.5/6.0
- Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2

FortiAuthenticator VM support options:

SKU	Description
FC1-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 500 USERS)
FC2-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 1100 USERS)
FC3-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 5100 USERS)
FC4-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 10100 USERS)
FC8-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 25100 USERS)
FC5-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 50100 USERS)
FC6-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 100100 USERS)
FC9-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 500100USERS)
FC7-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1 - 1M USERS)

FortiAuthenticator VM license information:

Technical Specification	VM-BASE	VM-100-UG	VM-1000-UG	VM-10000-UG	VM-100000-UG
Virtual CPUs (Maximum)	Unlimited				
Virtual Interfaces (Min / Max)	1 /4				
Virtual Memory (Min / Max)	512MB / 64GB				
Virtual Storage (Min / Max)	60GB / 2TB				
High Availability	Yes (Active-Passive HA and Config Sync HA)				
FortiTokens	200	+200	+2,000	+20,000	+200,000
NAS Devices / User Group	10	+10	+100	+1,000	+10,000
Local Users / Remote Users / User Certificates	100	+100	+1,000	+10,000	+100,000
CA Certificates	5	+5	+50	+500	+500

After placing an order for FortiAuthenticator VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiAuthenticator VM with Fortinet Customer Service & Support.

Upon registration, you can download the license file. You will need this file to activate your FortiAuthenticator VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded, the CLI and Web-based Manager are fully functional.

System requirements

Prior to deploying the FortiAuthenticator VM virtual appliance, either VMware vSphere Hypervisor (ESX versions 4.0 or 4.1, ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, or 6.0), Microsoft Hyper-V Server (2008R2 or 2012R2), or Virtual Machine Manager for KVM must be installed and configured. Note that, Virtual Machine Manager version 1.3.2 was used for the purposes of this document.

The installation instructions for FortiAuthenticator VM assume you are familiar with both VM platforms and their related terminology.

For more details on all platforms, refer to:

- http://www.vmware.com/products/vsphere-hypervisor/overview.html
- https://www.microsoft.com/en-ca/server-cloud/solutions/virtualization.aspx
- https://virt-manager.org/

Upgrade to the latest stable server update and patch release.

Note that FortiAuthenticator KVM is only supported on FortiAuthenticator version 4.3.

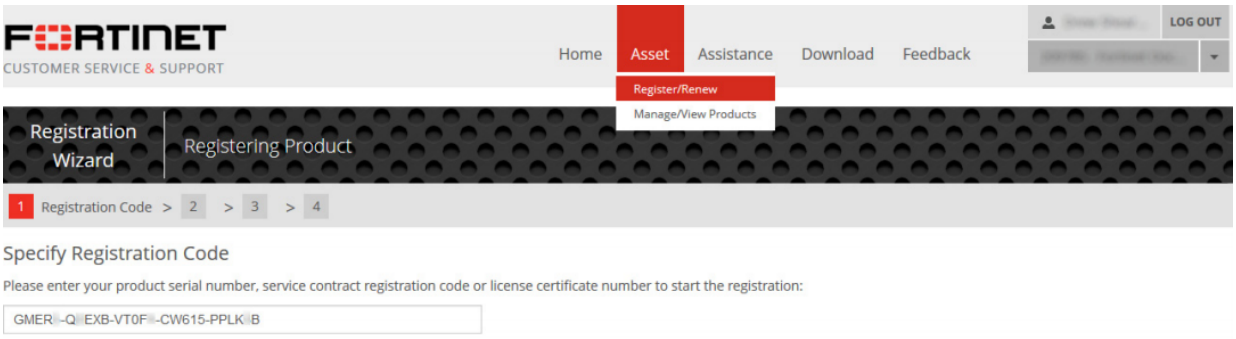
Register FortiAuthenticator VM with Customer Service and Support

To obtain the FortiAuthenticator VM license file you must first register your FortiAuthenticator VM with Fortinet Customer Service & Support.

To register your FortiAuthenticator VM:

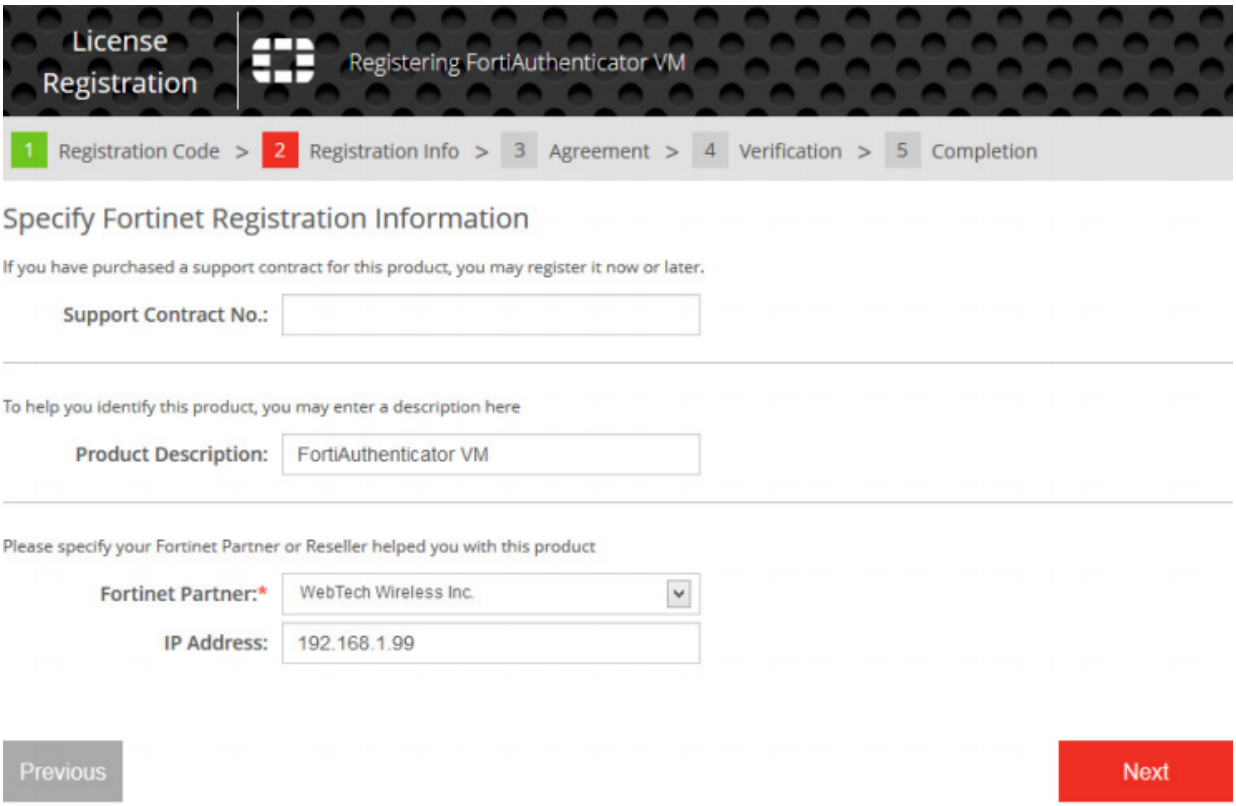
1. Log in to the Fortinet Customer Service & Support portal using an existing support account or select **Create an Account**.
2. In the toolbar select **Asset > Register/Renew**.
   The **Registration Wizard** opens.

   Figure 2: Registration Wizard



3. Enter the license registration code from the FortiAuthenticator VM License Certificate that was emailed to you and select **Next**. The **Registration Info** page is displayed.

Figure 3: Registration Info page



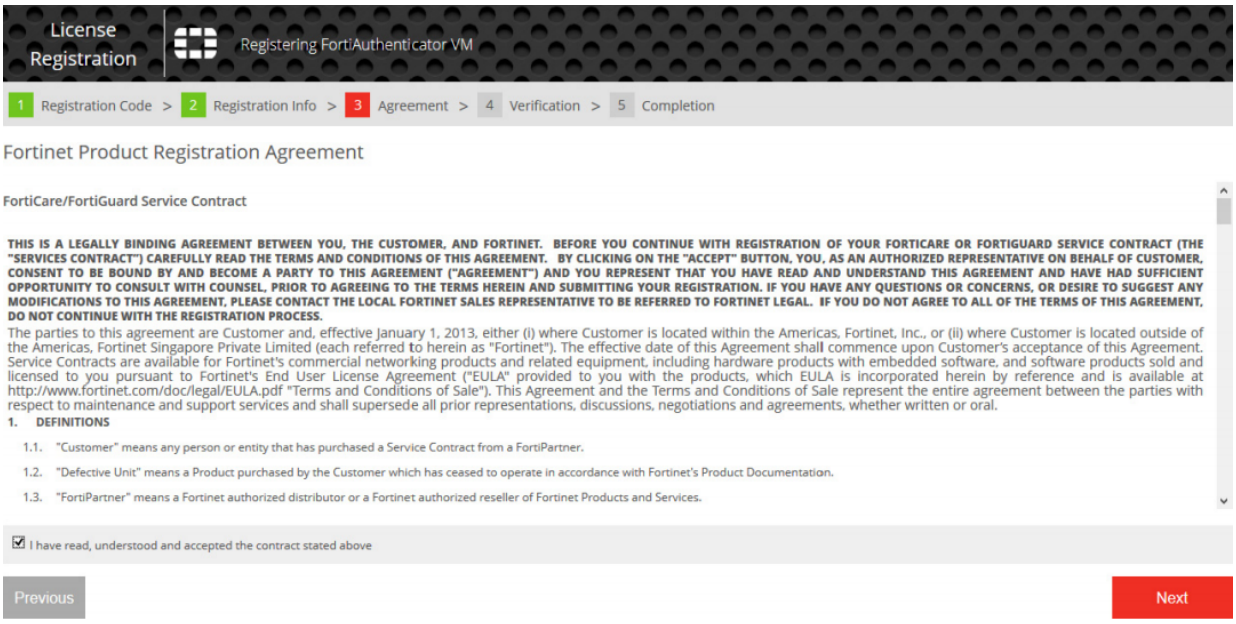
4. Enter the support contract number, product description, Fortinet Partner, and IP address.

As a part of the license validation process FortiAuthenticator VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAuthenticator VM's IP address has been changed, the FortiAuthenticator VM must be rebooted in order for the system to validate the change and operate with a valid license.

The Customer Service & Support portal currently does not support IPv6 for FortiAuthenticator VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

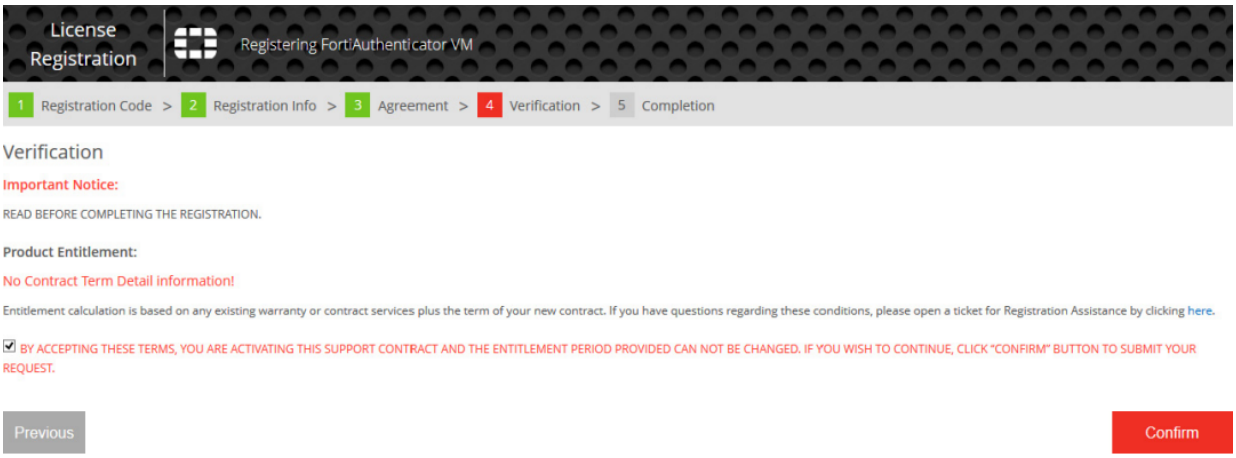
5. Select **Next** to continue. The **Fortinet Product Registration Agreement** page is displayed.

Figure 4: Fortinet Product Registration Agreement



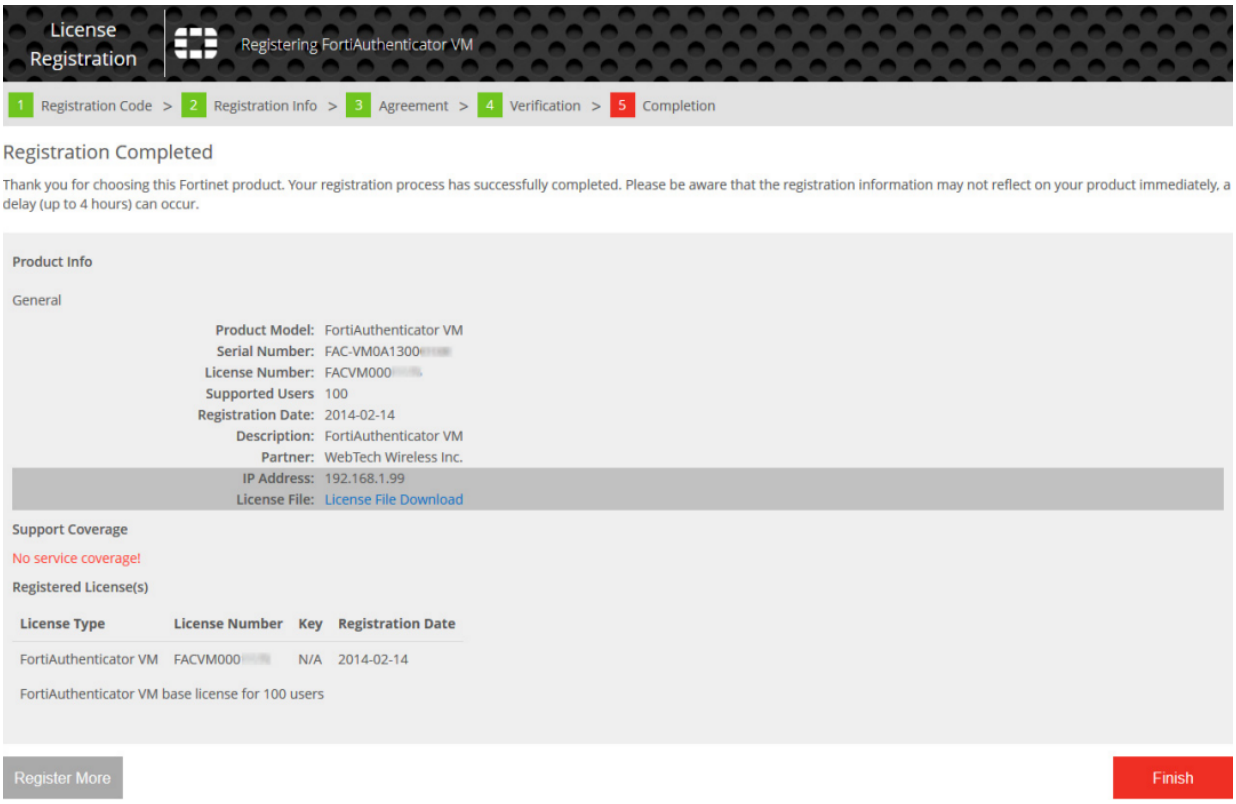
6. Select the check box to indicate that you have read, understood, and accepted the service contract, and select **Next** to continue. The **Verification** page is displayed.

Figure 5: Verification page



7. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms and select **Confirm** to submit the request. The **Registration Completed** page is displayed.

Figure 6: Registration Completed page

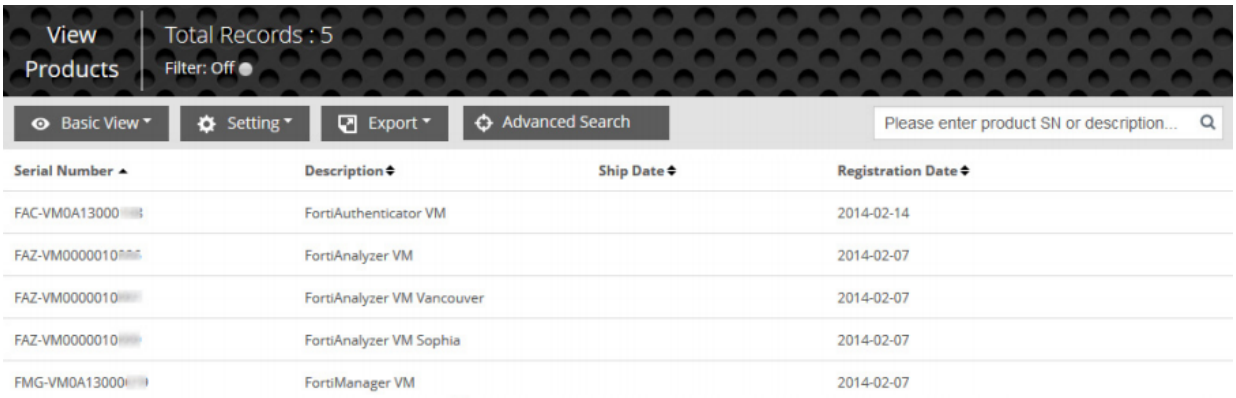


8. In the **Registration Completed** page you can download the FortiAuthenticator VM license file. Select the **License File Download** link. You will be prompted to save the license file (`.lic`) to your management computer. See "Upload the FortiAuthenticator VM license file" on page 1 for instructions on uploading the license file to your FortiAuthenticator VM via the Web-based Manager.

To edit the FortiAuthenticator VM IP address:

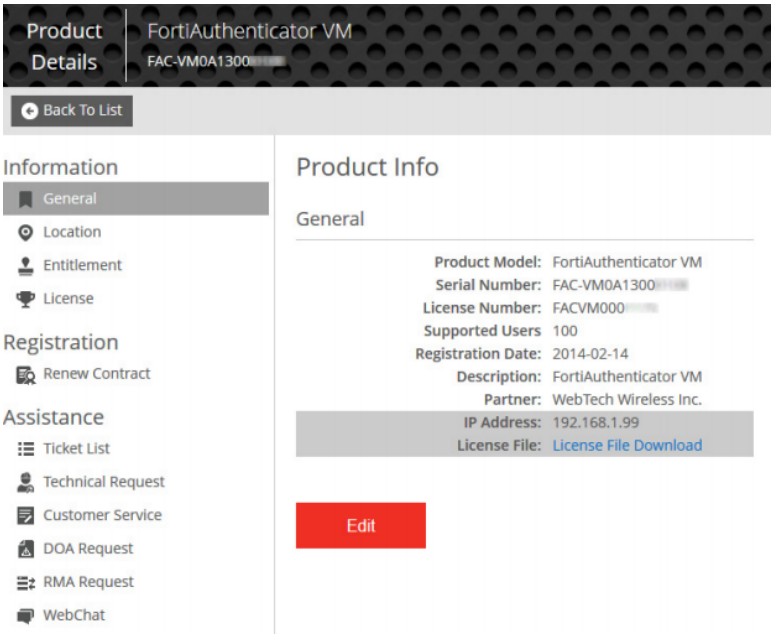
1. In the toolbar select **Asset > Manage/View Products**.
   The **View Products** page opens.

   Figure 7: View Products page



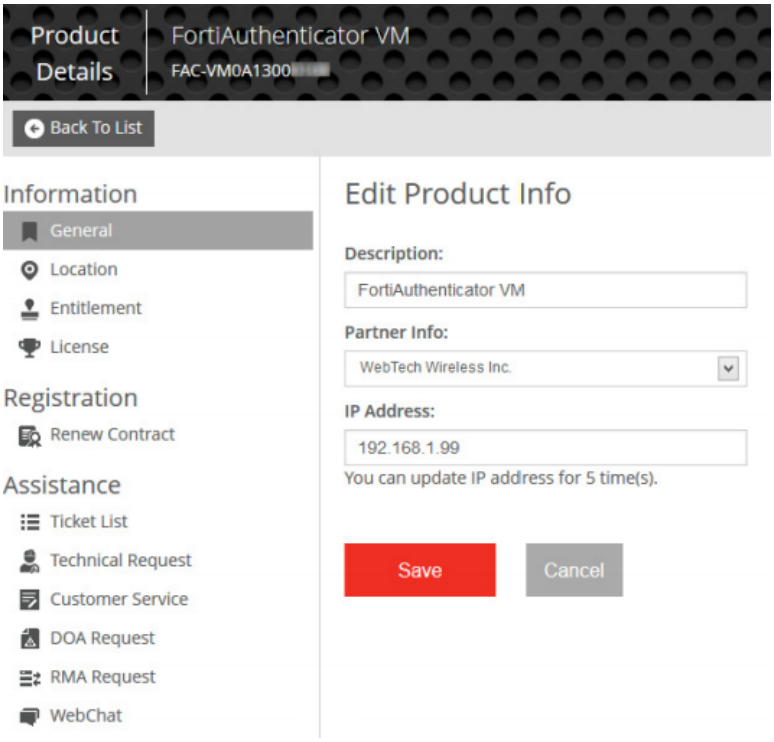
2. Select the FortiAuthenticator VM serial number.
   The **Product Details** page opens.

Figure 8: Product Details page



3. Select **Edit** to change the description, partner information, and IP address of your FortiAuthenticator VM. The **Edit Product Info** page opens.

Figure 9: Edit Product Info page



4. Enter the new IP address and select **Save**.

You can change the IP address five (5) times on a regular FortiAuthenticator VM license. There is no restriction on a full evaluation license.

5. Select the **License File Download** link. You will be prompted to save the license file (`.lic`) to your management computer. See "Upload the FortiAuthenticator VM license file" on page 1 for instructions on uploading the license file to your FortiAuthenticator VM via the Web-based Manager.

Download the FortiAuthenticator VM software

Fortinet provides the FortiAuthenticator VM software for 64-bit environments in two formats:

- FAC_VM-v300-build0xxx-FORTINET.out: Download this firmware image to upgrade your existing FortiAuthenticator VM installation.
- FAC_VM-v300-build0xxx-FORTINET.out.ovf.zip: Download this package for a new FortiAuthenticator VM installation.

The zip file is available in hyperv and OVF formats, for MS Hyper-V and VMware ESXi respectively. The .out file can upgrade both.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site.

MS Hyper-V deployment package contents

The **FAC_VM_HV-v400-buildxxxx-FORTINET.out.hyperv.zip** file contains:

- **Snapshots folder**:
  - Optionally, Hyper-V stores snapshots of the FortiAuthenticator VM state here.
- **Virtual Hard Disks folder**:
  - DATADRIVE.vhd: The FortiAuthenticator VM log disk in VHD format.
  - fac.vhd: The FortiAuthenticator VM system hard disk in VHD format.
- **Virtual Machines folder**:
  - fortiauthenticator.xml: XML file containing virtual hardware configuration settings for Hyper-V.

VMware ESXi deployment package contents

The **FAC_VM-v400-buildxxxx-FORTINET.out.ovp.zip** file contains:

- datadrive.vmdk: The FortiAuthenticator VM log disk in VMDK format.
- fac.vmdk: The FortiAuthenticator VM system hard disk in VMDK format.
- FortiAuthenticator-VM.ovf: OVF template file for VMware Hardware Type 10 (intel E1000 NIC Driver).
- FortiAuthenticator-VM.hw04.ovf: OVF template file for VMware Hardware Type 10 (intel E1000 NIC Driver).
- FortiAuthenticator-VM.hw07.ovf: OVF template file for VMware Hardware Type 10 (intel E1000 NIC Driver).

The FAC_VM-v300-build0xxx-FORTINET.out.ovf.zip file contains the following files:

- datadrive.vmdk: Virtual machine disk format file used by the OVF file.
- fac.vmdk: Virtual machine disk format file used by the OVF file.
- FortiAuthenticator-VM.hw04.ovf: Open Virtualization Format file for VMware ESX 4.0 environments that support hardware version 4.
- FortiAuthenticator-VM.hw07_vmxnet2.ovf: Open Virtualization Format file for VMware ESX 4.0 environments that support hardware version 7.
- FortiAuthenticator-VM.ovf: Open Virtualization Format file for VMware.

KVM deployment package contents

The **FAC_VM_KVM-v400-build0216-FORTINET.out.kvm.zip** file contains the following QCOW2 and XML files:

- datadrive.qcow2
- fackvm.file
- fackvm.xml
- fackvm.qcow2
- README.file

FortiAuthenticator VM firmware images in the Fortinet Customer Service & Support portal FTP directory are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FAC_VM-v300-build0004-FORTINET.out.ovf.zip image found in the v3.0 directory is specific to the FortiAuthenticator VM VMware environment.

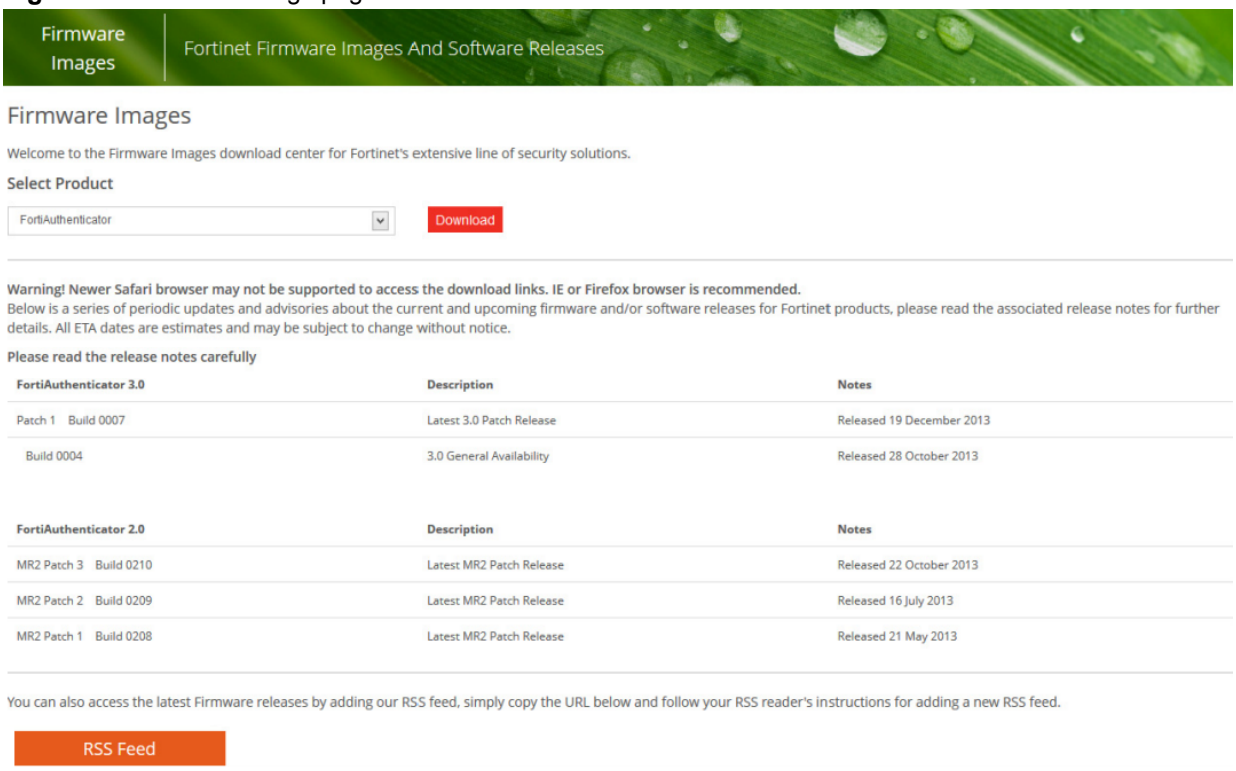
You can download the FortiAuthenticator Release Notes available on the Fortinet web site.

Note that the download steps below are for VMWare specifically. For MS Hyper-V, download the .hyperv.zip deployment package.

To download the FortiAuthenticator VM .ovf.zip package:

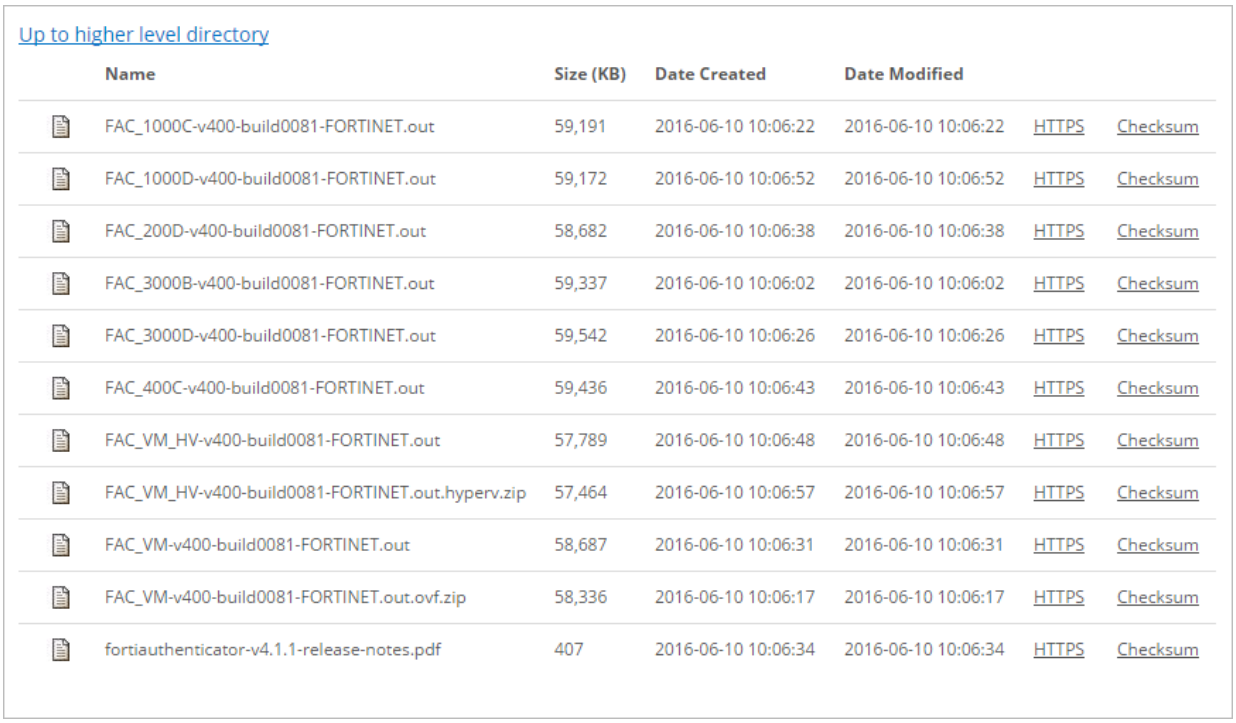
1. Log into the Fortinet Customer Service & Support portal, select **Download** in the toolbar, and select **Firmware Images** from the drop-down list.
   The **Firmware Images** page opens.

Figure 10: Firmware image page



2. In the **Firmware Images** page, select **FortiAuthenticator**.
3. Browse to the appropriate directory in the FTP site for the version that you would like to download.

Figure 11: FTP directory example



4. Download the `.ovf.zip` file and FortiAuthenticator Release Notes, and save these files to your management computer.
5. Select the `.ovf.zip` file on your management computer and extract the files to a new file folder. See "Deploy the FortiAuthenticator VM OVF file" on page 1 for information on deploying the OVF file to your VMware environment.

FortiAuthenticator VM evaluation license

FortiAuthenticator VM includes a 5-user evaluation license. No activation is required for the built-in evaluation license and there is no expiration of this license.

Technical support is not included with evaluation license.

Please contact your Fortinet Reseller should you require an extended evaluation i.e. with more users.

FortiAuthenticator VM Deployment

For best performance, it is recommended that FortiAuthenticator VM is installed on a “bare metal” hypervisor (such as VMware ESXi or MS Hyper-V). Hypervisors that are installed as applications on top of a general purpose operating system (such as Microsoft Windows, Mac OS X, or Linux) will have fewer computing resources available due to the host OS’s own overhead.

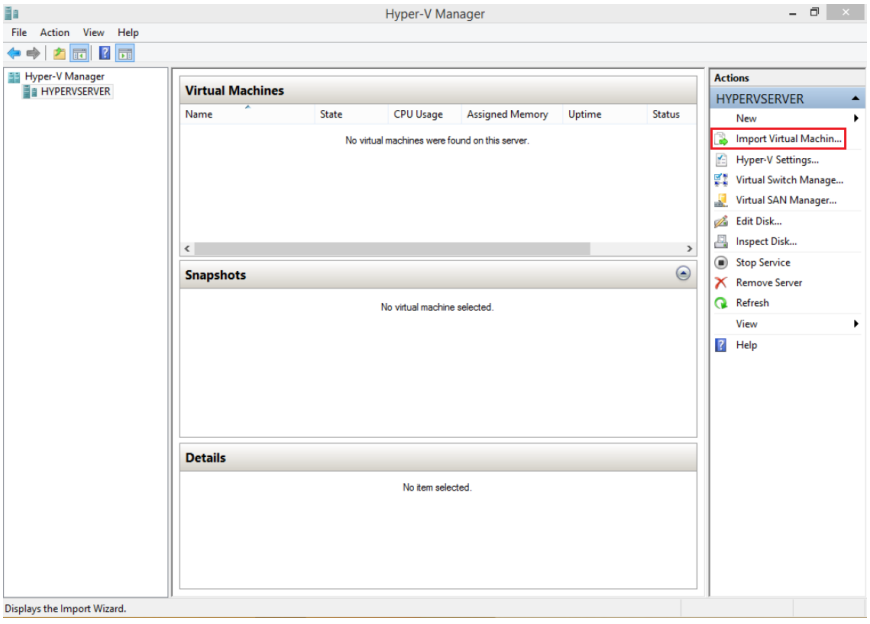
The following sections detail deployments for MS Hyper-V, VMware ESX/ESXi, and Linux Virtual Machine Manager:

Deployment example: MS Hyper-V

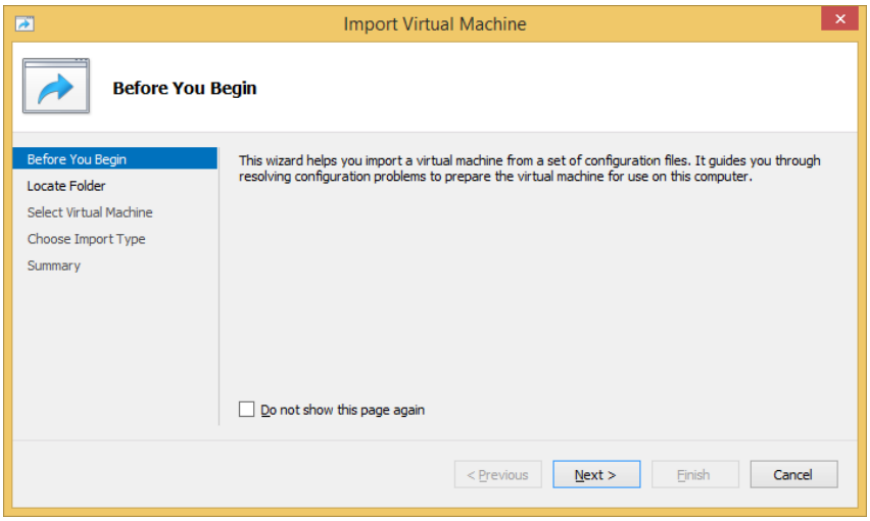
Once you have downloaded the `out.hyperv.zip` file and extracted the package contents to a folder on your management computer, you can deploy the VHD package to your MS Hyper-V environment.

To deploy the FortiAuthenticator VHD template:

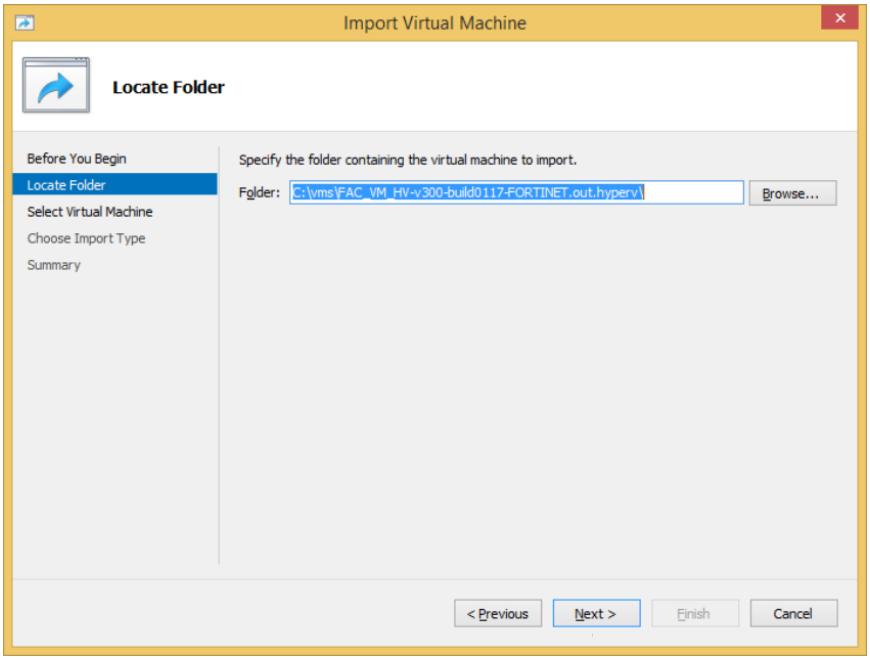
1. As an Administrator, launch the Hyper-V Manager and connect to your Hyper-V Server.
2. Select the server in the right-hand menu and select **Import Virtual Machine**.



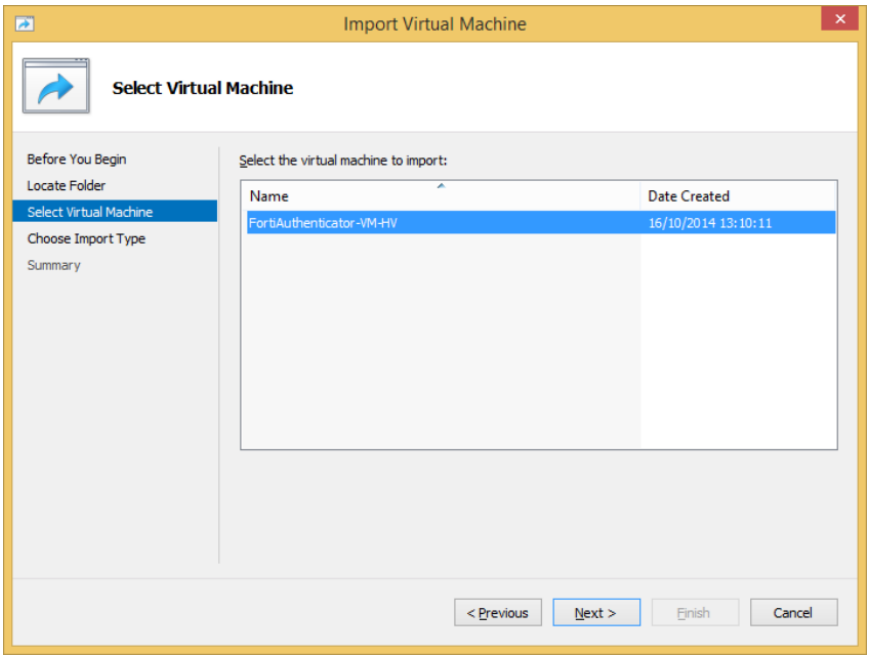
The **Import Virtual Machine** page opens. Select **Next** to begin the VM Import process.



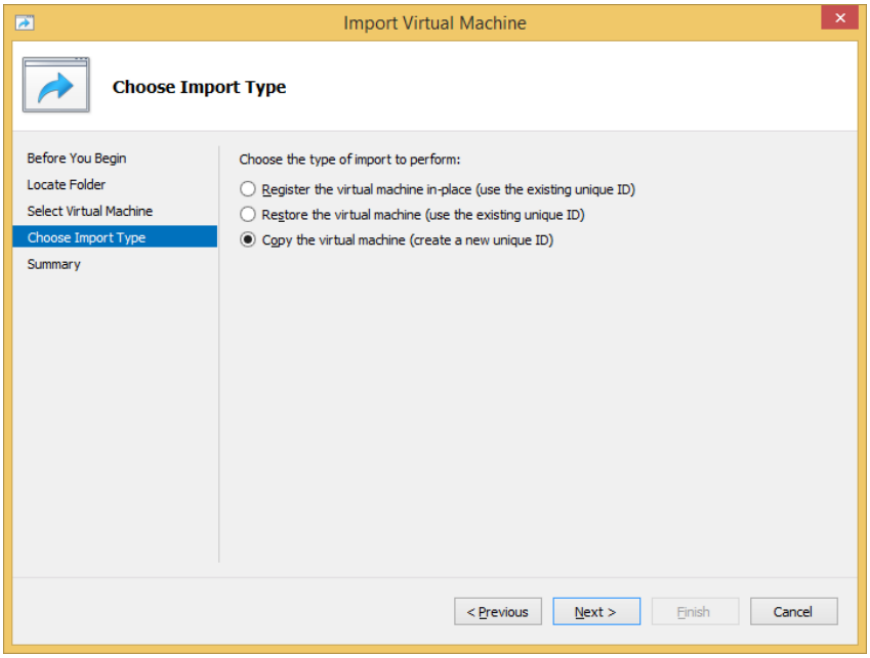
3. Enter the location of the VM to be imported. This is the location of the folder that you extracted the FortiAuthenticator `hyperv.zip` file to.



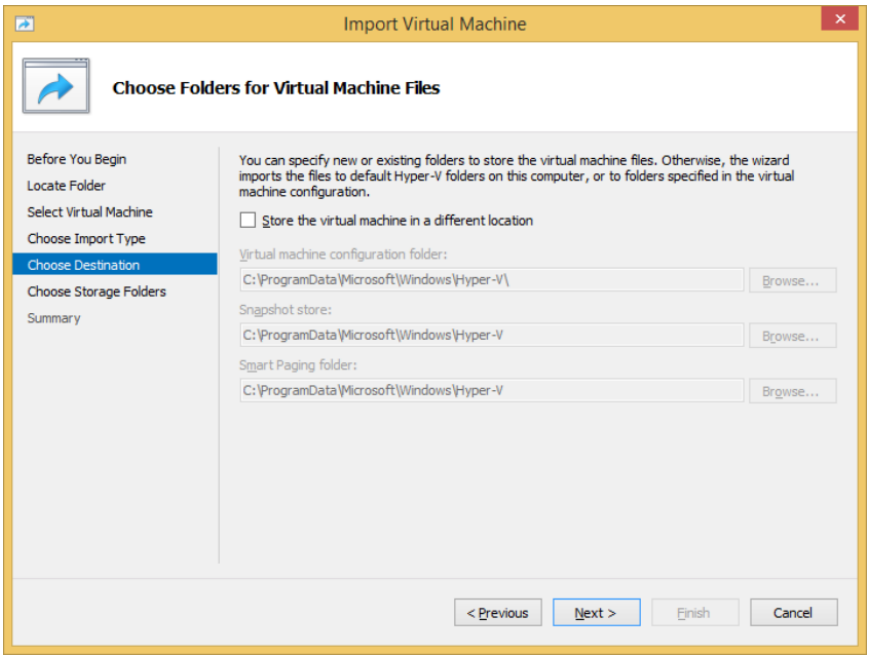
4. Select the FortiAuthenticator VM and select **Next**.



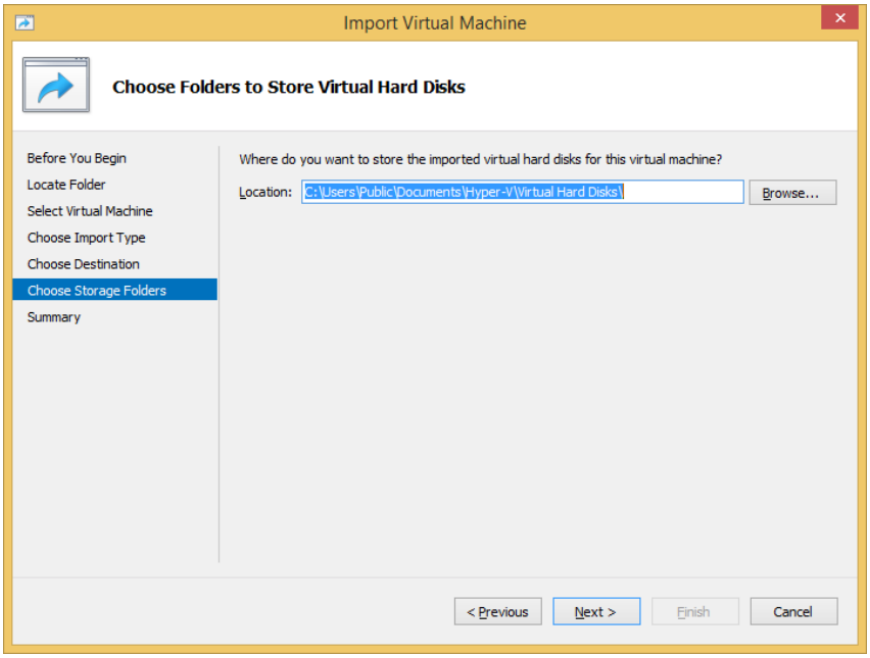
5. For the import type, choose **Copy the virtual machine** and select **Next**.



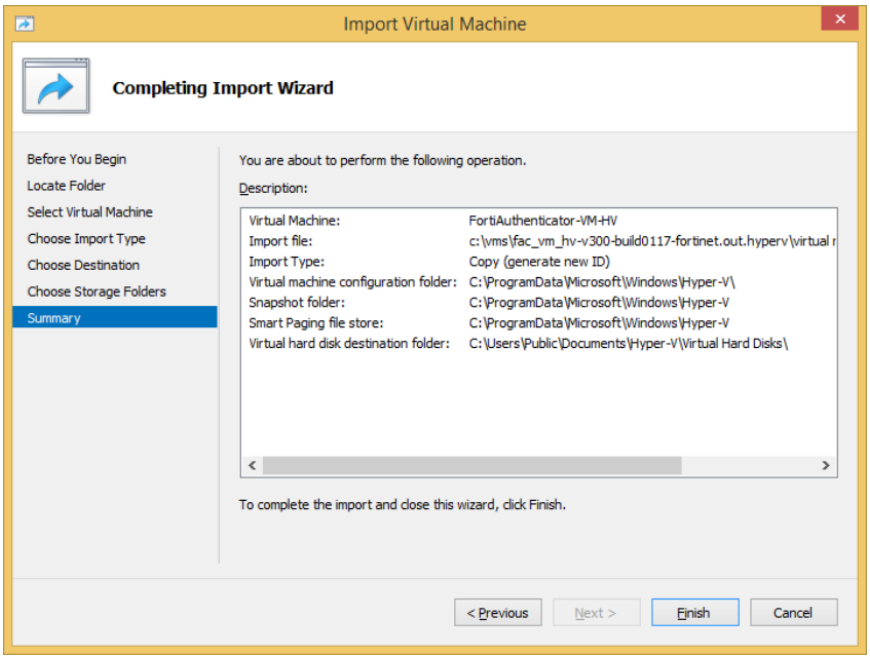
6. Select **Next** if you wish to use the default storage location settings, or specify your own.



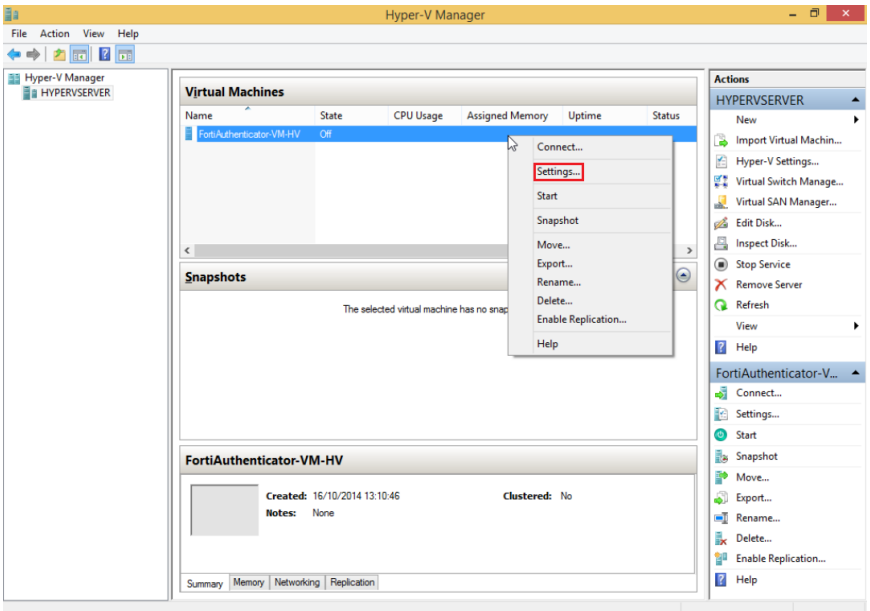
7. Select **Next** if you wish to use the default VM hard disk storage settings, or specify your own.



8. Select **Finish** to accept the configuration and complete the VM installation.



9. The VM will be installed and will be displayed in the Hyper-V Manager. Once complete, and before the VM is started, the hardware settings can be modified. Right-click the new VM and select **Settings...**.



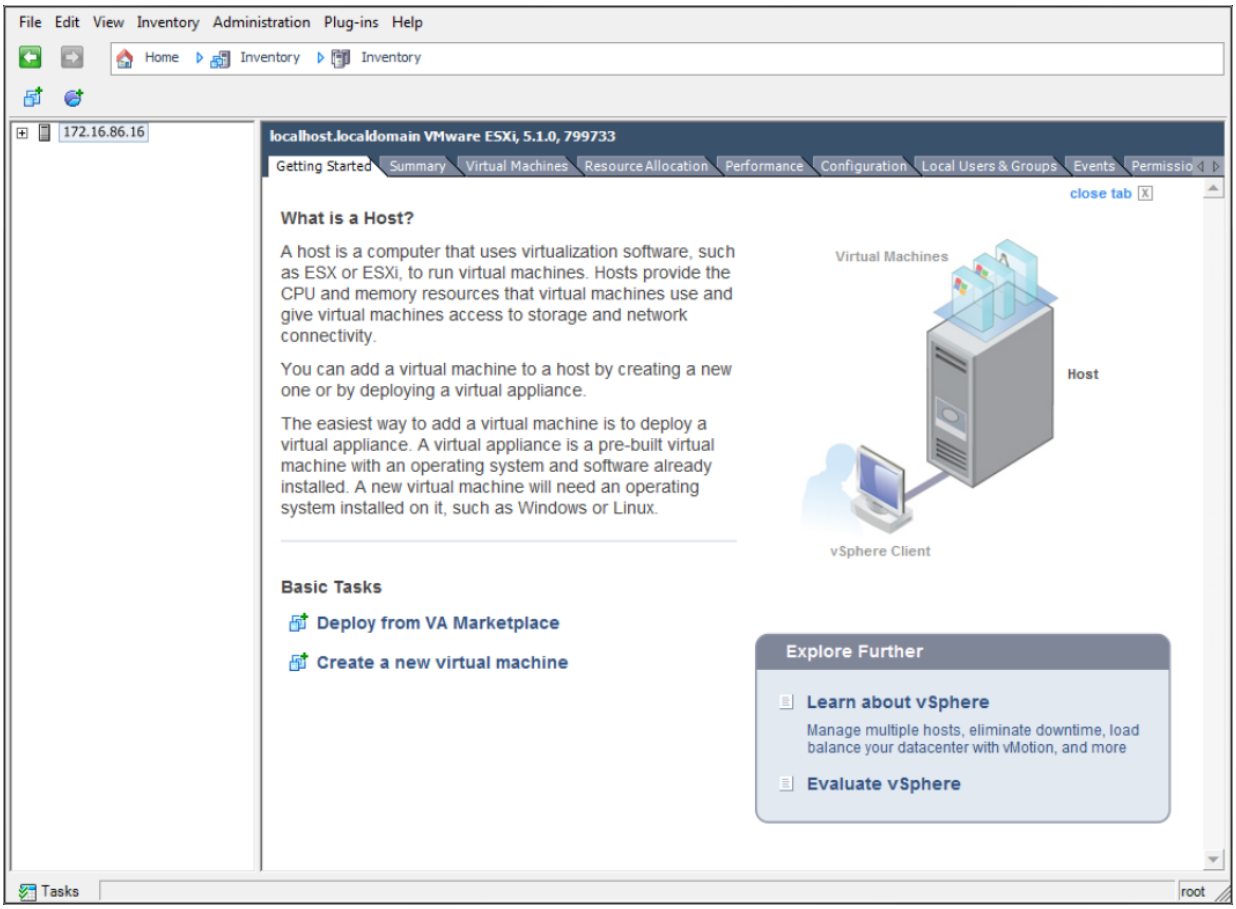
Deployment example: VMware

Once you have downloaded the `out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

To deploy the FortiAuthenticator VM OVF template:

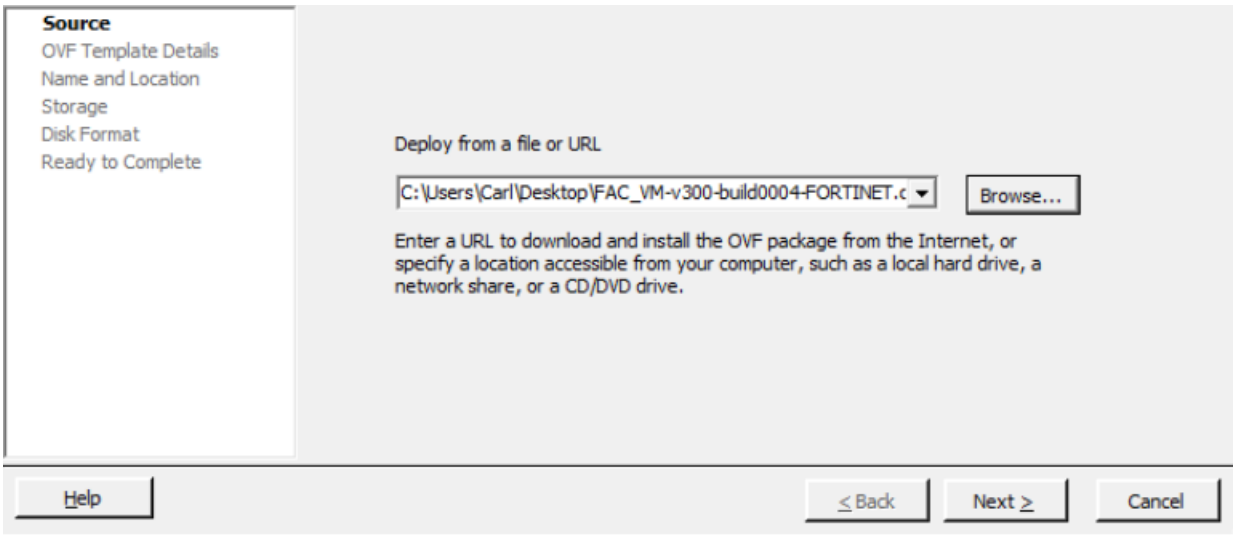
1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, and select **Login**.
   The vSphere client home page opens.

   Figure 12: vSphere client home page



2. Select **File > Deploy OVF Template** to launch the OVF Template wizard.
   The **Source** page opens.

   Figure 13: Source page

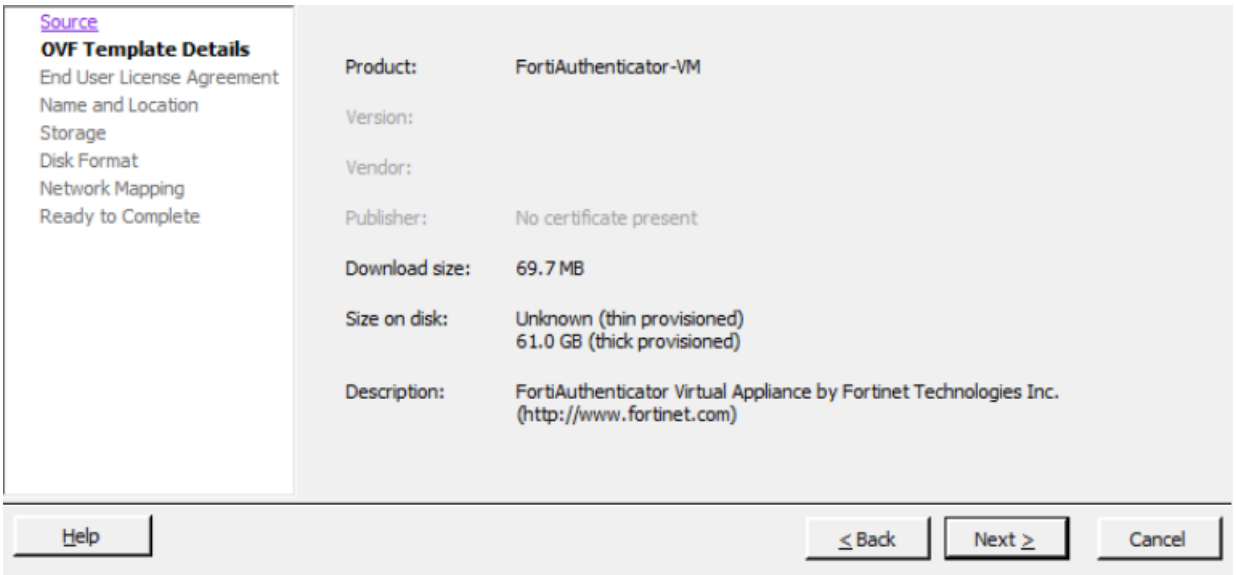


3. Select the source location of the OVF file. Select **Browse** and locate the file folder on the management computer. Select the appropriate FortiAuthenticator VM OVF file and select **Next** to continue.

Select the FortiAuthenticator-VM.ovf file and it will select the most appropriate OVF format (hw07_vmxnet2.ovf or hw04.ovf) based on your hardware and server version.

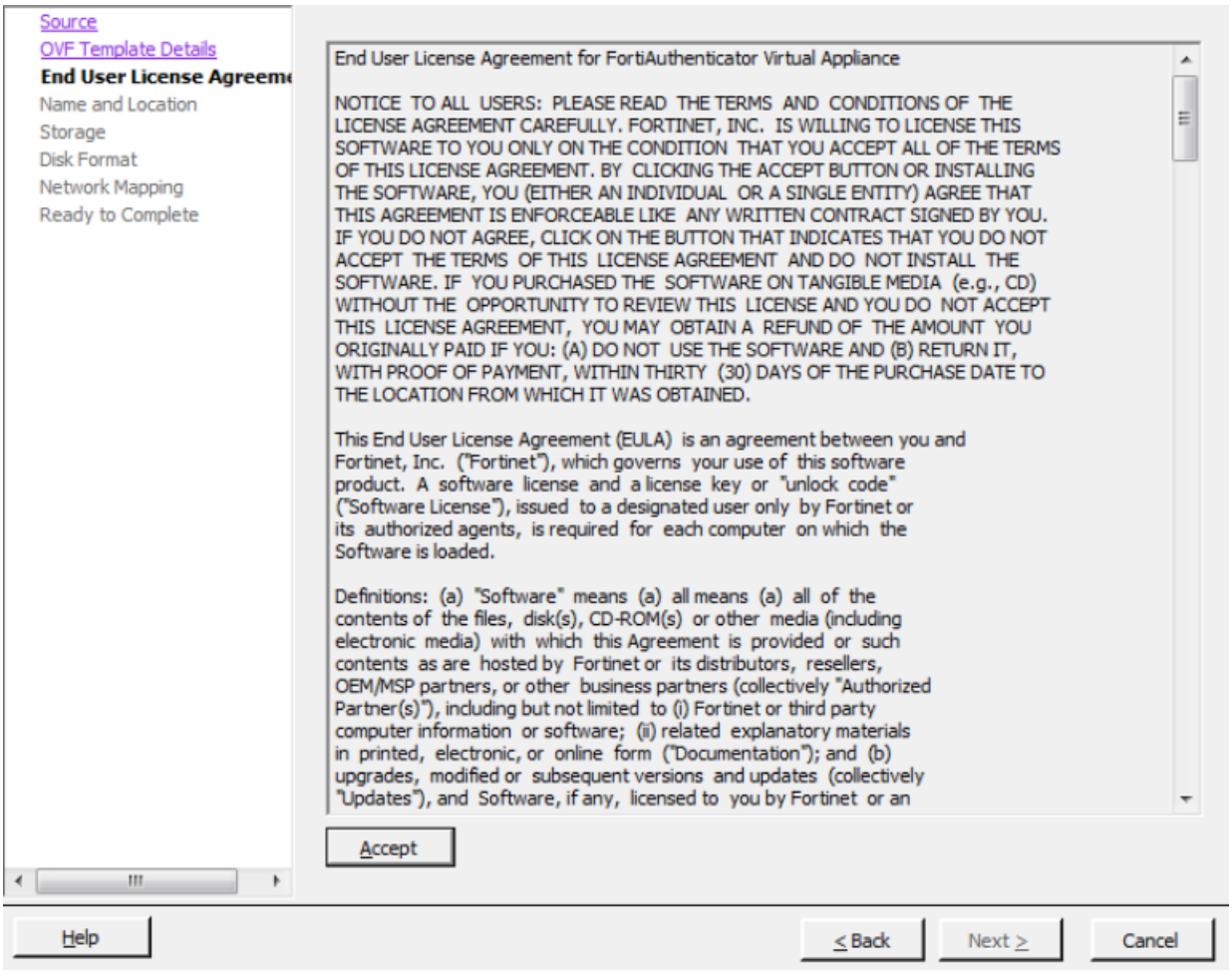
The **Details** page opens.

Figure 14: OVF Template Details page



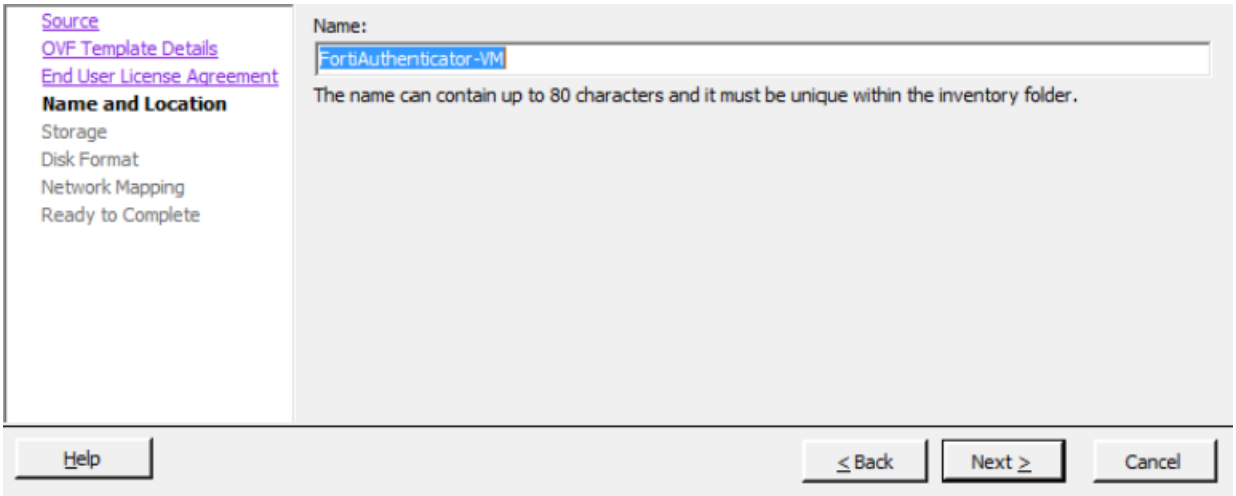
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select **Next** to continue.
The **End User License Agreement** page opens.

Figure 15: End User License Agreement page



5. Read the end user license agreement for FortiAuthenticator VM. Select **Accept** and then select **Next** to continue. The **Name and Location** page opens.

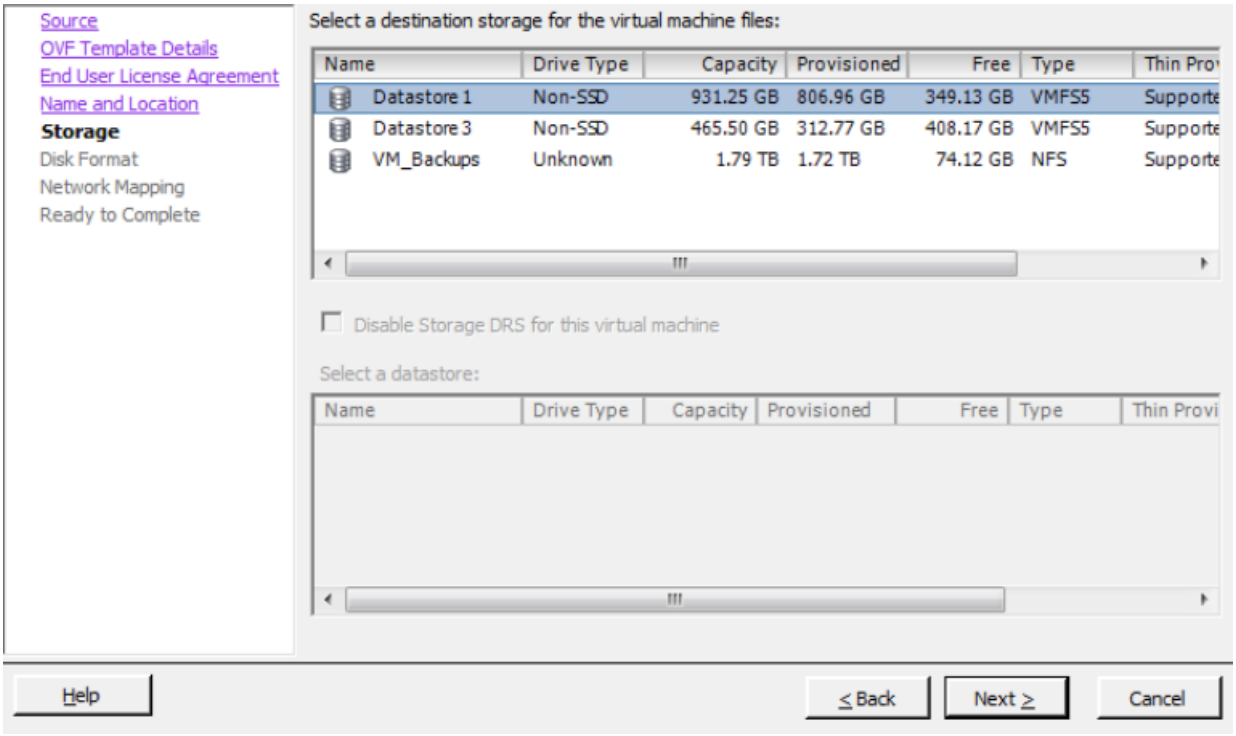
Figure 16: Name and Location page



6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select **Next** to continue.

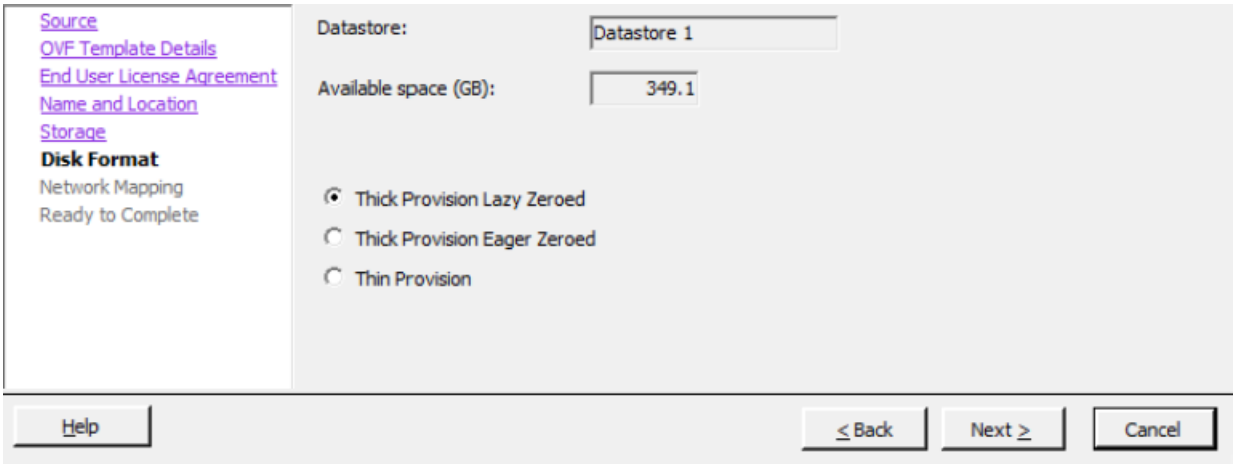
The **Storage** page opens.

Figure 17: Storage page



7. Select where you want to store the virtual machine files. Select **Next** to continue.
The **Disk Format** page opens.

Figure 18: Disk Format page



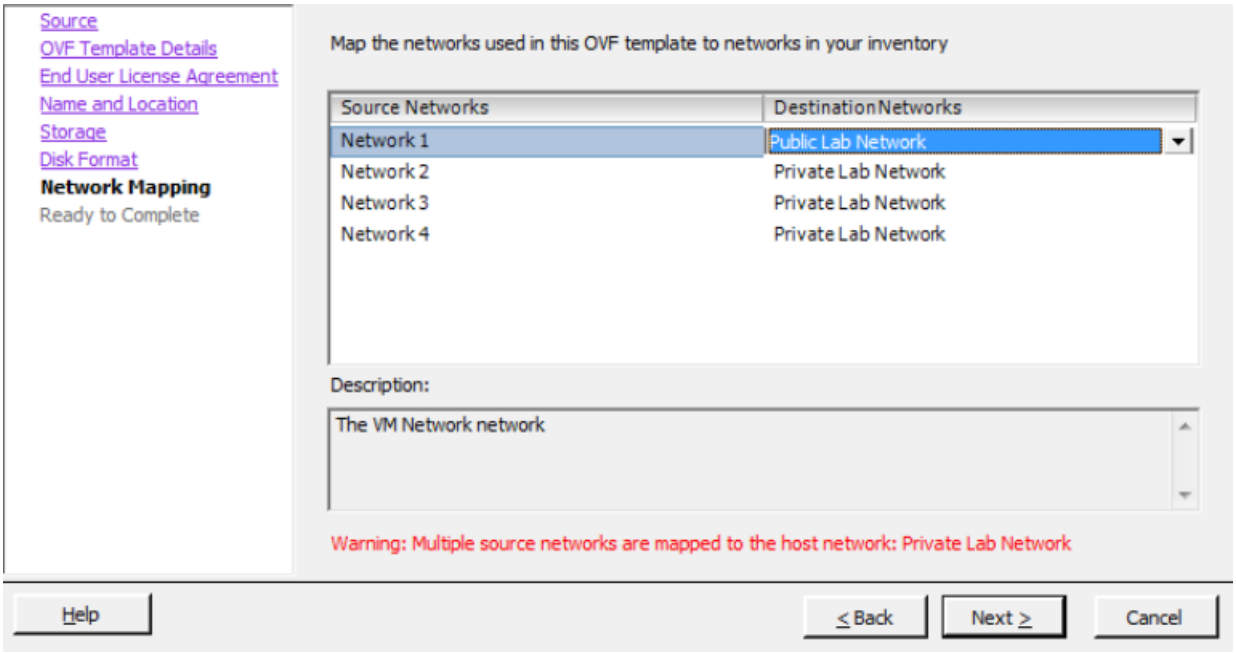
8. Select one of the following:
   - **Thick Provision Lazy Zeroed:** Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - **Thick Provision Eager Zeroed:** Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.

- **Thin Provision:** Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless if you have deleted data, etc.

The best choice depends on your virtualization environment. The most optimal method is to deploy in Thick Provisioned Format because the disk space is allocated at time of the installation. Thin provisioning has the benefit of using less disk space initially. However, performance is decreased, and issues can occur if the disk becomes filled with other VM instances.

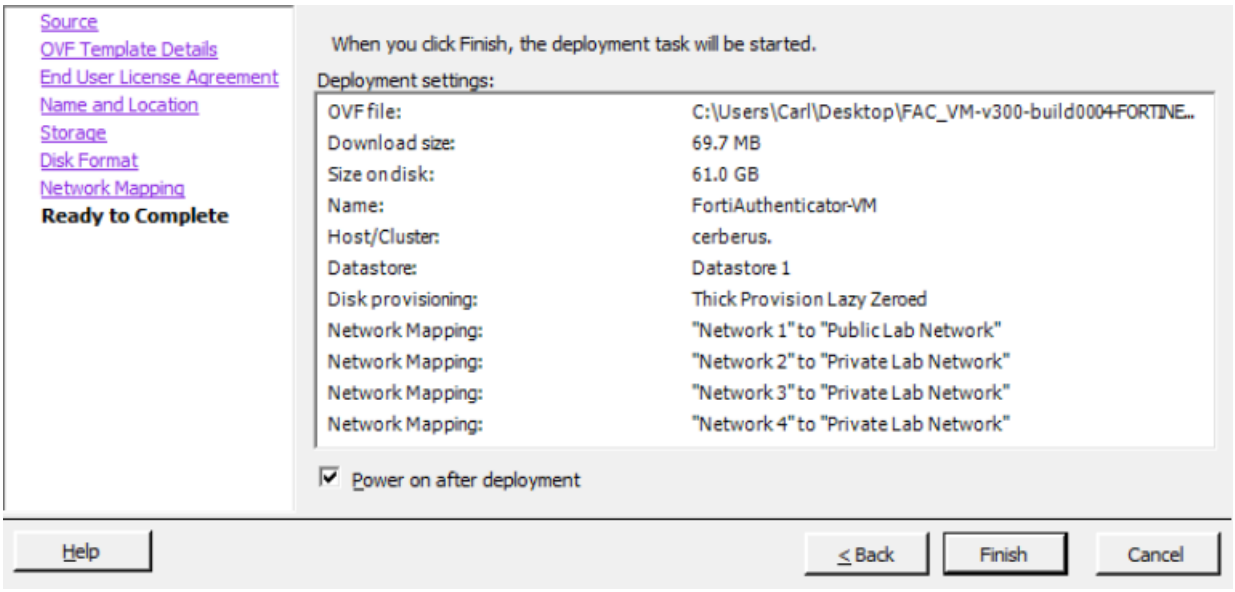
Select **Next** to continue.
The **Network Mapping** page opens.

Figure 19: Network Mapping page



9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiAuthenticator VM. You must set the destination network for this entry to access the device console. Select **Next** to continue.
The **Ready to Complete** page opens.

Figure 20: Ready to Complete page



10. Review the template configuration. To power on the FortiAuthenticator VM select the checkbox beside **Power on after deployment**.

It is recommended to configure the FortiAuthenticator VM hardware settings prior to powering on the FortiAuthenticator VM.

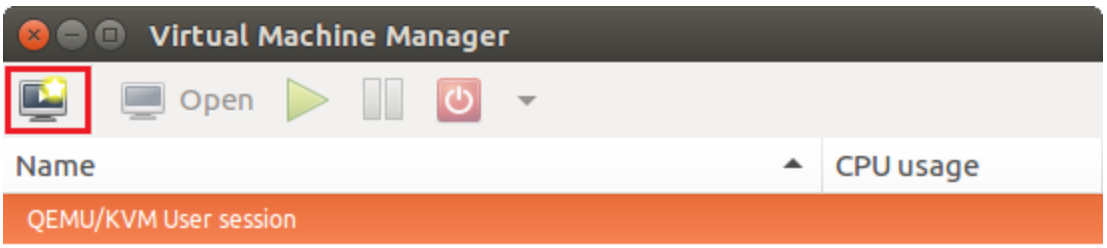
11. Select **Finish** to deploy the OVF template. You will receive a **Deployment Completed Successfully** dialog box once the FortiAuthenticator VM OVF template wizard has finished.

Deployment example: KVM

Once you have downloaded the `out.kvm.zip` file and extracted the virtual hard drive image file fackvm.qcow2, you can create the virtual machine in your KVM environment.

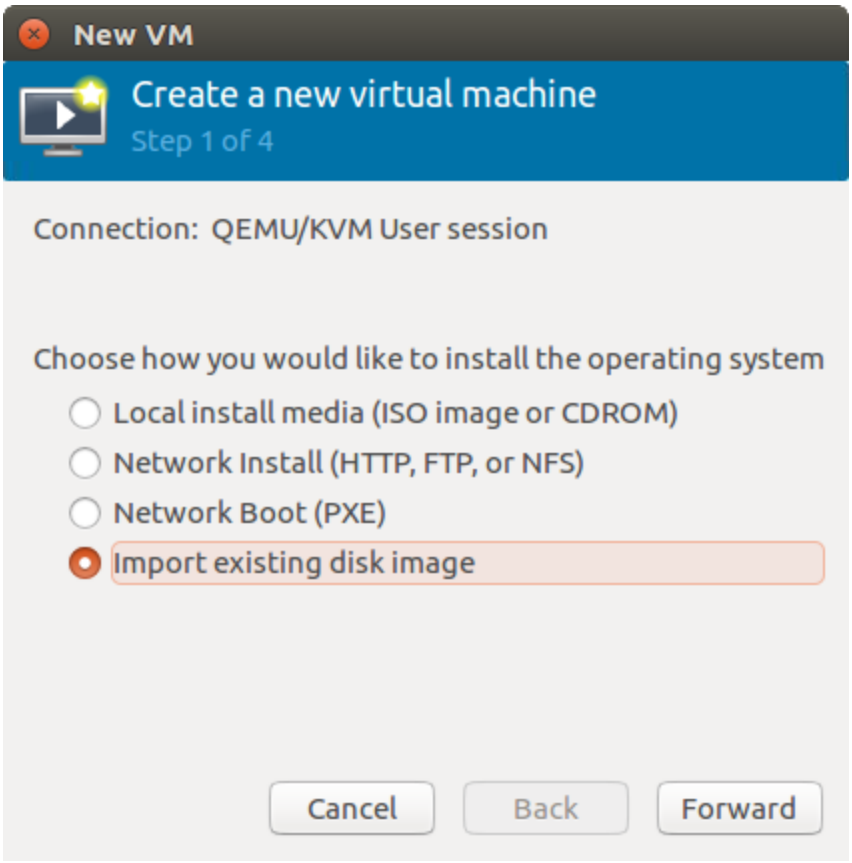
To deploy the FortiAuthenticator VM virtual machine:

1. Launch **Virtual Machine Manager** on your KVM host server.
2. From the Virtual Machine Manager (VMM) home page, select **Create a new virtual machine**.

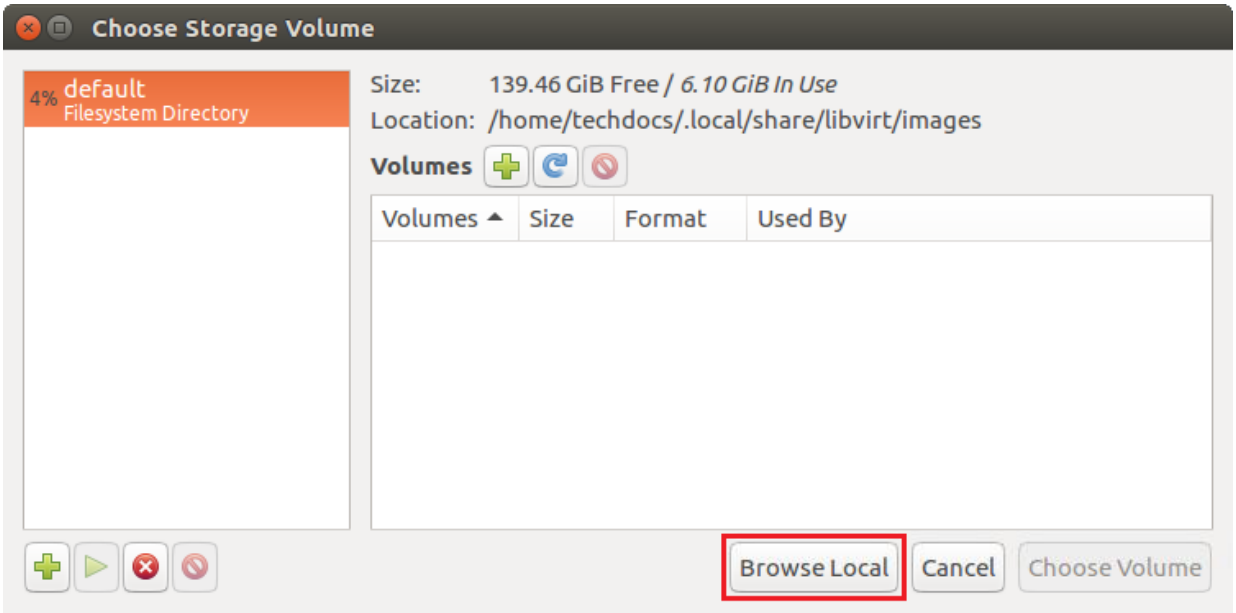


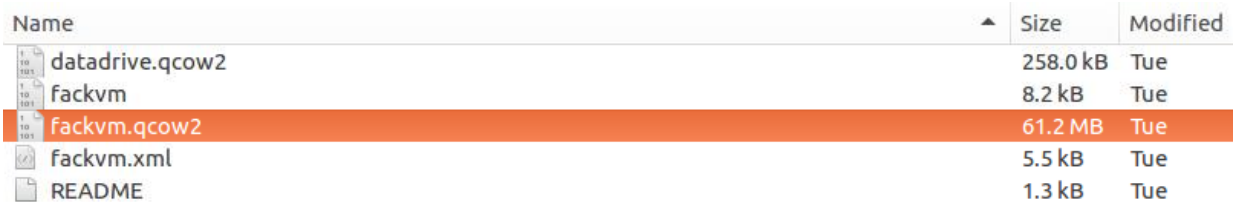
The **New VM** window will open.

3. Select **Import existing disk image** and select **Forward**.

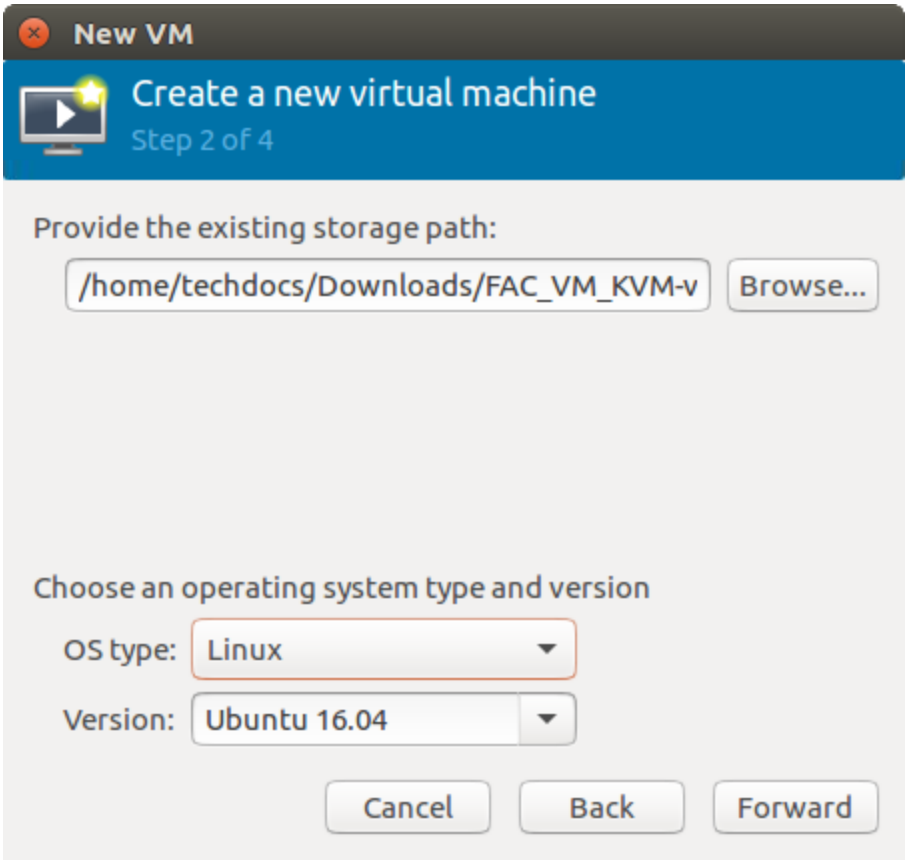


4. Select **Browse**. If you saved the **fackvm.qcow2** file to **/var/lib/libvirt/images**, it will be visible on the right. If you saved it somewhere else on your server, select **Browse Local**, find it, and select **Choose Volume**.

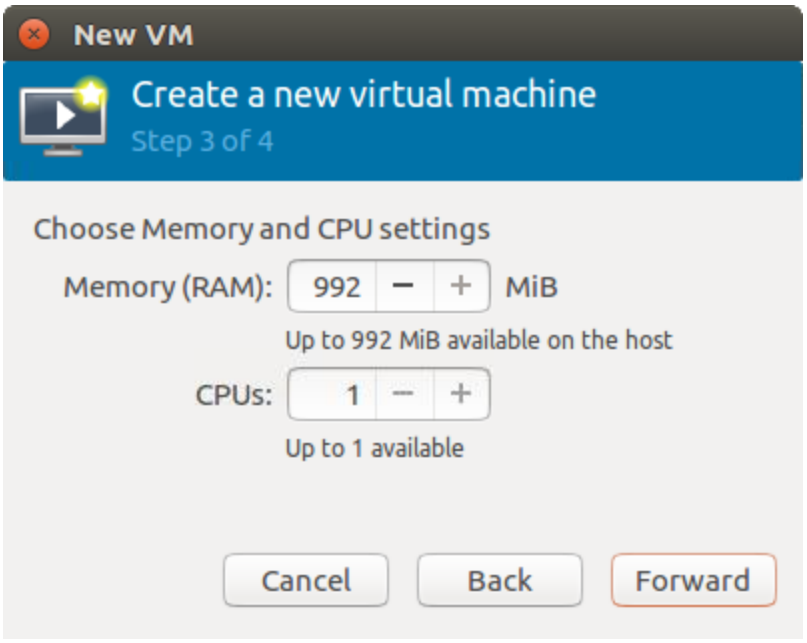




5. Select the **OS type** and **Version** you are running (in this case **Linux Ubuntu 16.04**), and select **Forward**.

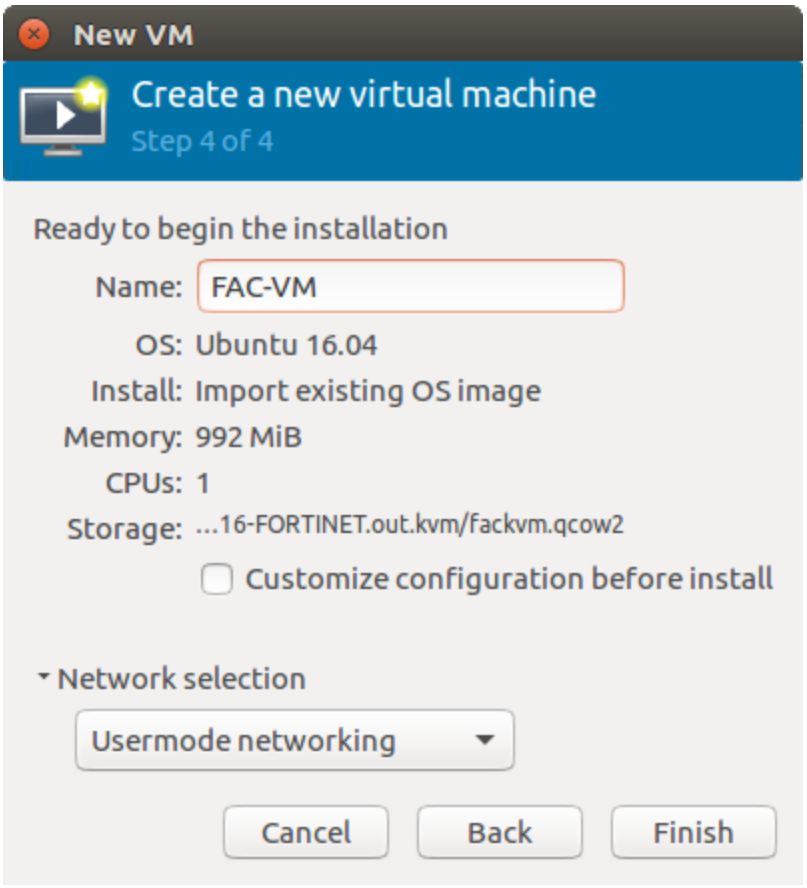


6. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. For more information on your license limits, see Licensing.



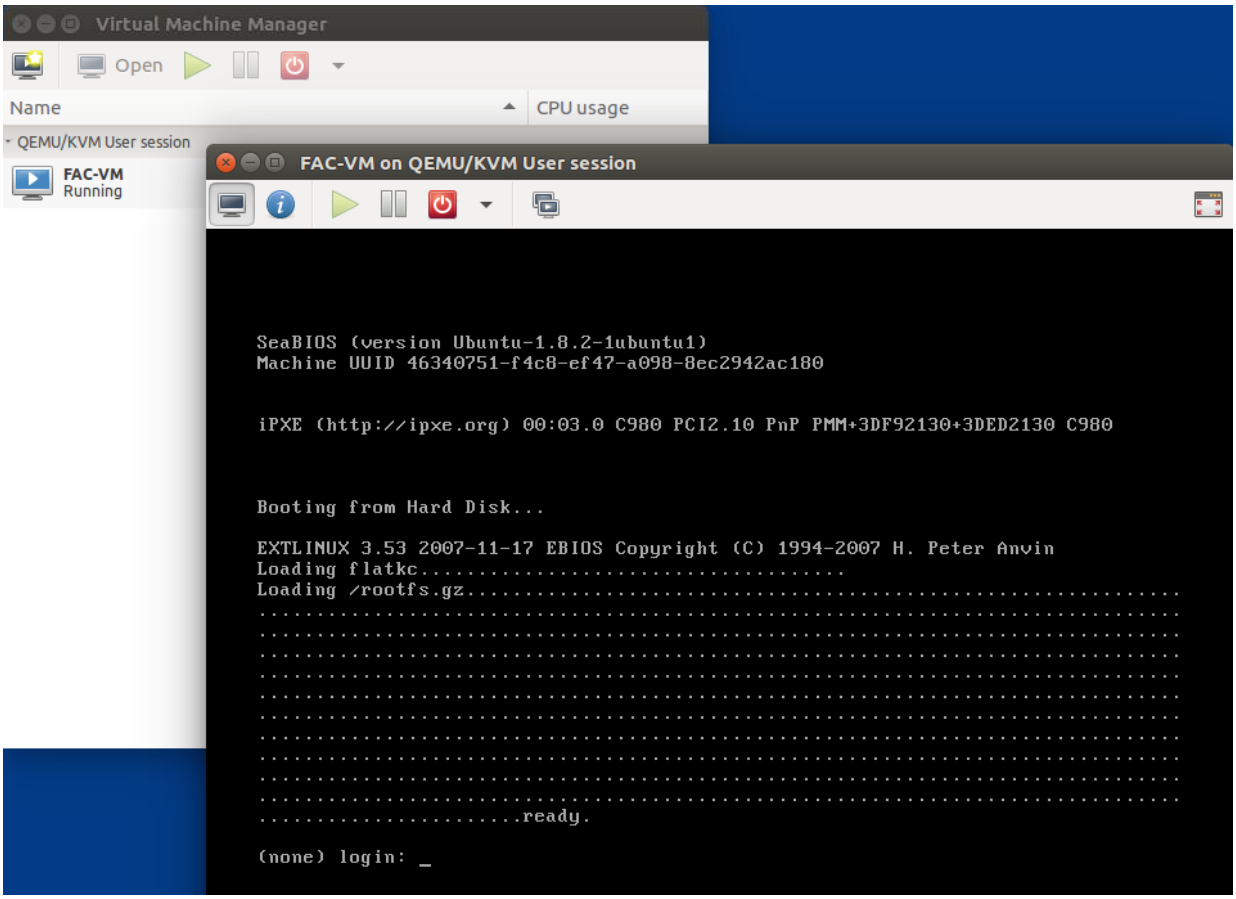
Then select **Forward**.

7. On the last page, enter a **Name** for the VM (in this case, **FAC-VM**).
   A new virtual machine includes one network adapter by default. Set **Network selection** to **Usermode networking**. Alternatively, set a specific MAC address for the virtual network interface by selecting **Specify shared device name**.



Then select **Finish**.

You new VM will be created an open, prompting login.



Resizing the virtual disk

To resize the disk, and adjust partitions, you must set up the libvirt guest filesystem utilities. The command used to resize the disk, on an Ubuntu host with qcow2 file images, is `virt-resize`.

Import factors to know about this method are the following:

- This is a libvirt utility
- It can both expand a guest disk and expand the partitions at the same time
- It copies the disk, which is beneficial if you wish to keep a backup.

Install utilities package

1. Open the VMM **Terminal** and enter the following command to install the libvirt file system utilities package:
   `sudo apt-get install libguestfs-tools`
2. To see if the libvirt utility is functional, you will need to run a test. Enter the following command:
   `sudo apt-get install libguestfs-tools`
   If you see `===== TEST FINISHED OK =====`, it is functional.
3. If you don't see the successful test-finished command return, you will need to repair it. In this case, enter the following command:
   `sudo update-guestfs-appliance`
4. Run the test again (the command from step 2) to verify that it works.

Resize disk and partition

1. First of all, shutdown the guest VM.
2. Review the current sizing and view the partition name you want to expand by using the following libvirt utility command:
   ```
   sudo virt-filesystems --long --parts --blkdevs -h -a <name-of-guest-disk-file>
   ```
3. Enter the following command to increase the output disk size. This example increases the disk size by 20GB:
   ```
   sudo qemu-img create -f qcow2 -o preallocation=metadata outdisk 20G
   ```
4. Enter the following command to copy the old disk to the new disk, while expanding the suitabkle partition:
   ```
   sudo virt-resize --expand <name-of-partition> indisk outdisk
   ```
5. When finished, make sure to rename the indisk file to an appropriate name, such as "backup", while you rename the new outdisk as "indisk".
6. Reboot the guest and test the new disk. When a successful test is complete, you are free to delete the original backup file if you wish.

Configuring the number of virtual CPUs

By default, the virtual appliance is configured to use one (1) virtual CPU (vCPU).

To change the number of vCPUs:

1. First of all, shutdown the guest VM.
2. Right-click the VM and go to **Open > Show virtual hardware details > CPUs**.
3. Under **Topology**, enable **Manually set CPU topology** and select the number of virtual **Sockets**, the number of **Cores** per socket, and number of **Threads**.
4. Select **Apply** to save the settings.

Configuring the memory limit

VMM measures its memory by mebibytes (MiB).

To change the memory limit:

1. First of all, shutdown the guest VM.
2. Right-click the VM and go to **Open > Show virtual hardware details > Memory**.
3. Enter the **Maximum allocation** in MiB to allocate to the VM instance.
4. Select **Apply** to save the settings.

Configure FortiAuthenticator VM hardware settings

Before powering on your FortiAuthenticator VM you must configure the virtual memory, virtual CPU, and virtual disk (VMDK) configuration, and map the virtual network adapters.

These settings cannot be configured inside FortiAuthenticator VM, and must be configured in the VM environment. Some settings cannot be reconfigured after you power on the virtual appliance.

To see information on how to similarly configure FAC KVM on an Ubuntu host running Virtual Machine Manager, see Resizing the virtual disk and other sections in the KVM deployment example.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance's storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk before powering on.

This step is not applicable if the virtual appliance will use external network file system (such as NFS) datastores.

The FortiAuthenticator VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files of 1GB for disk 1 (for the OS) and 60GB for disk 2 data, which is large enough for most small deployments. This can be extended if necessary. Resize the vDisk before powering on the virtual machine.

Before doing so, make sure that you understand the effects of your vDisk settings.

During the creation of a VM datastore, you have the following formatting options:

- 1MB block size - 256GB maximum file size
- 2MB block size - 512GB maximum file size
- 4MB block size – 1,024GB maximum file size
- 8MB block size – 2,048GB maximum file size

These options affect the possible size of each vDisk.

For example, if you have an 800GB datastore which has been formatted with 1MB block size, you cannot size a single vDisk greater than 256GB on your FortiAuthenticator VM.

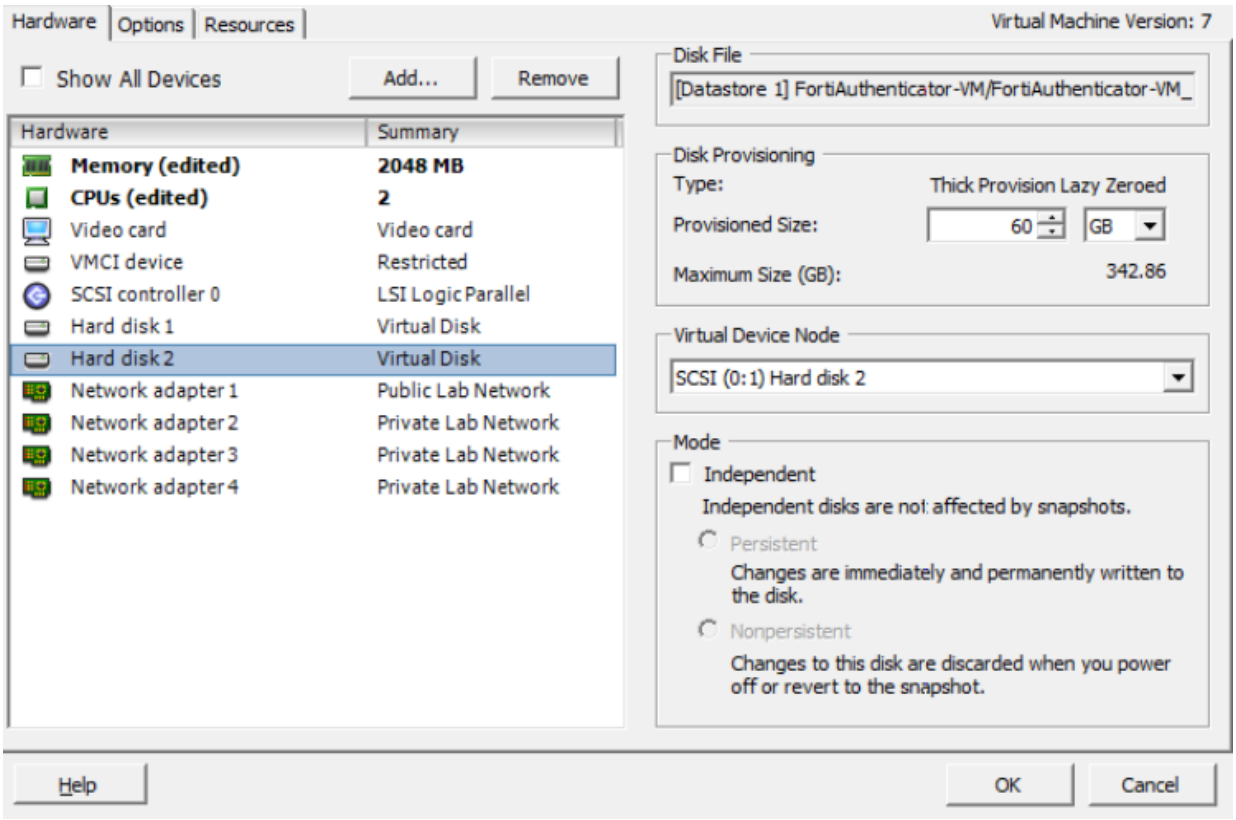
Consider also that, depending on the size of your organization's network, you might require more or less storage for the user database and logging.

For more information on vDisk sizing, see http://communities.vmware.com/docs/DOC-11920.

To resize the vDisk:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select **Edit Settings**. The **Virtual Machine Properties** page is displayed.

   Figure 21: Virtual Machine Properties



2. Select the **Hardware** tab and select Hard Disk 2.
3. Select **Remove**.
4. Select **Add**.
   The **Add Hardware** page is displayed.
5. In the list of device types, select **Hard Disk** and select **Next**.
6. Select **Create a new virtual disk** and select **Next**.
7. In **Disk Size**, enter the size of the vDisk in GB and select **Next**.
8. Select the bottom option in **Virtual Device Node**, select **IDE (0:1)** from the drop-down list, then select **Next**.
9. Select **Finish** to close the **Add Hardware** page and then select OK to save the settings to Virtual Machine Properties.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 2 vCPUs. FortiAuthenticator VM is not restricted to how many vCPUs can be configured so you can increase the number according to your requirements e.g., you can allocate 2, 4, or 8 vCPUs.

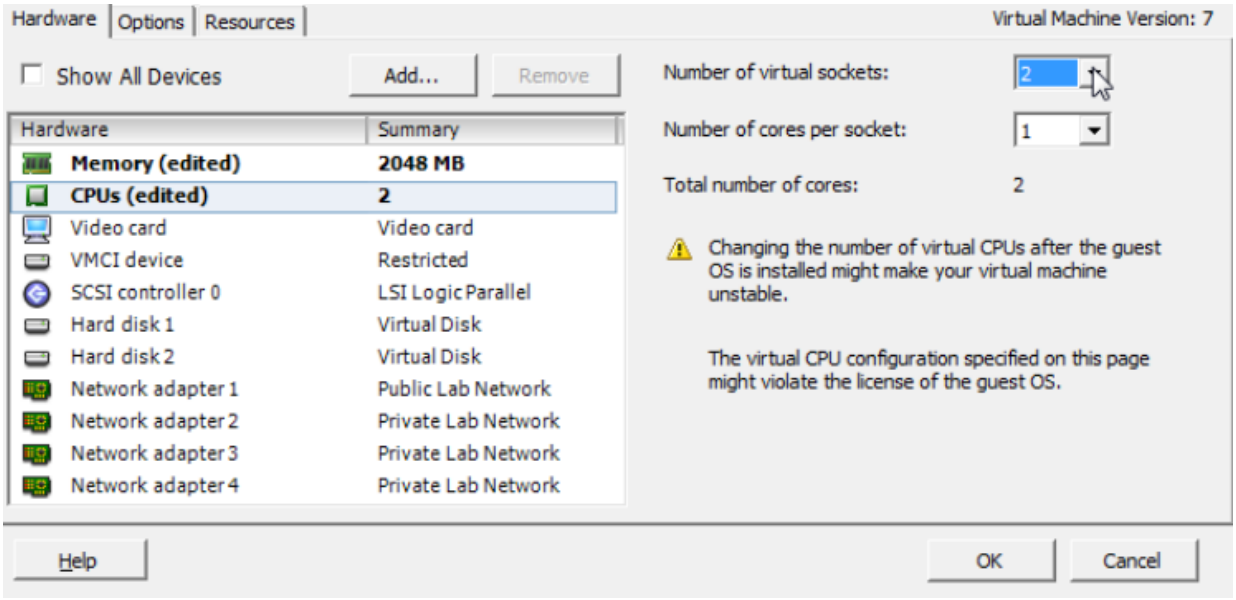
If you need to increase or decrease the vCPUs after the initial boot, power off FortiAuthenticator VM, adjust the number of vCPUs, then power on the VM.

For more information on vCPUs, visit http://www.vmware.com/products/vsphere-hypervisor/index.html for VMware vSphere documentation.

To change the number of vCPUs:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select **Edit Settings**. The **Virtual Machine Properties** page is displayed.

   Figure 22: VirtuAl Machine Properties



2. Select the **Hardware** tab and select CPUs.
3. Select the number of virtual sockets and the number of cores per socket.
4. Select **OK** to save the settings to Virtual Machines Properties.

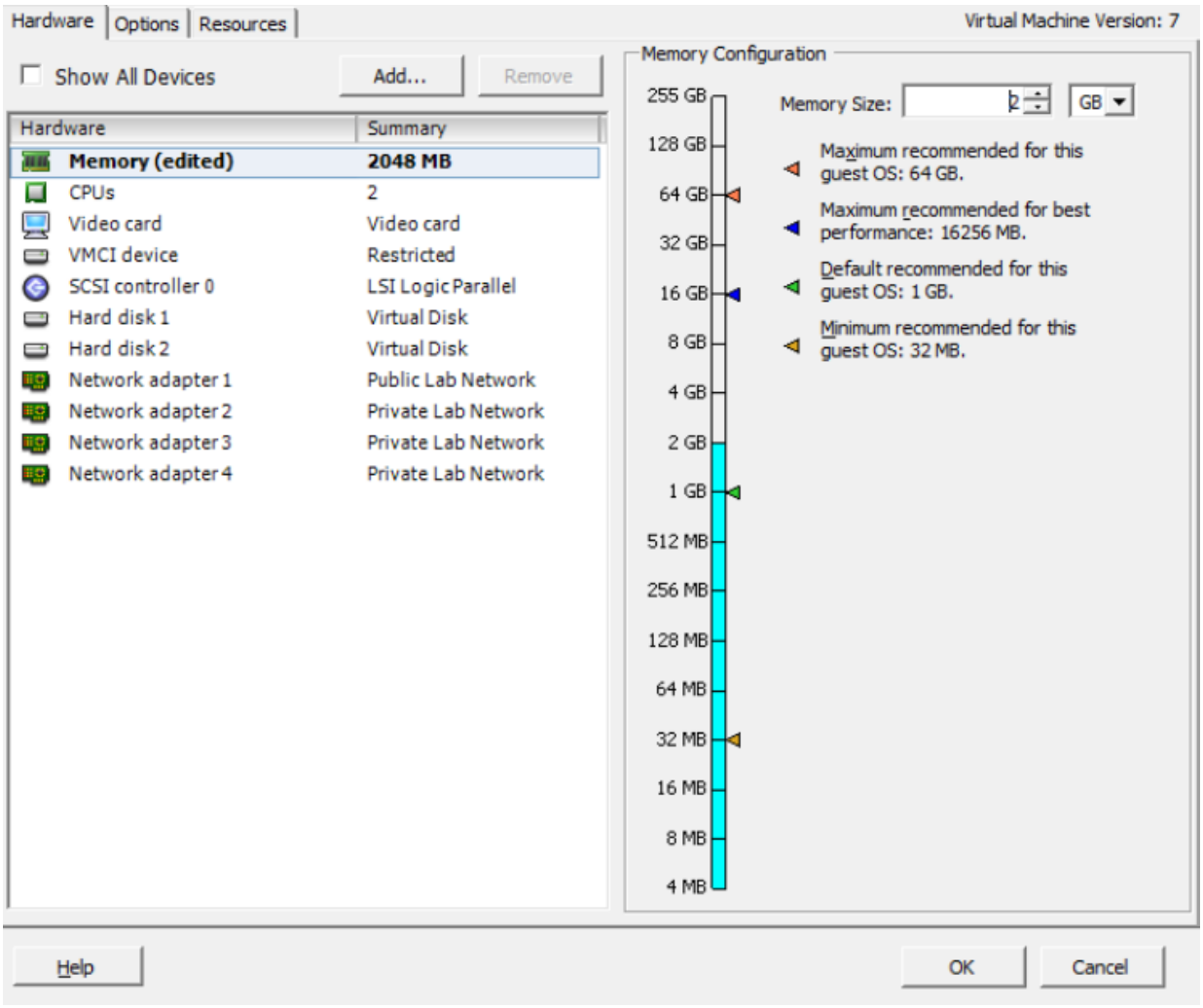
Configuring the virtual RAM (vRAM) limit

FortiAuthenticator VM comes pre-configured to use 512MB of vRAM. You can change this value. The valid range is from 512MB to 16GB.

To change the amount of vRAM:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select **Edit Settings**. The **Virtual Machine Properties** page is displayed.

   Figure 23: Virtual Machine Properties



2. Select the **Hardware** tab and select **Memory**.
3. Enter the maximum memory in GB to allocate to the VM instance.
4. Select **OK** to save the settings to Virtual Machine Properties.

Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiAuthenticator VM ports to physical ports depends on your existing virtual environment. Often, the default bridging vNICs work, and do not need to be changed.

If you are unsure of your network mappings, try bridging first before non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network. The most common exceptions to this rule are for VLANs and the transparent modes.

When you deploy the FortiAuthenticator VM package, 4 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 4 network interfaces in FortiAuthenticator VM.

Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC. vSwitches are themselves mapped to physical ports on the server.

Example network mapping:

VMware vSphere			FortiAuthenticator VM
Physical Network Adapter	**Network Mapping (vSwitch Port Group)**	**Virtual Network Adapter for FAC VM**	**Network Interface Name in GUI and CLI**
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
eth0	VM Network 2	Internal (LDAP)	port3
eth0	VM Network 1	Unconfigured	port4

To map network adapters:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select **Edit Settings**. The **Virtual Machine Properties** page is displayed.
2. Select the **Hardware** tab and select Network adapter 1.
3. From the Network Connection drop-down list, select the virtual network mapping for the virtual network adapter. Repeat this step for the other 3 network adapters. The correct mapping varies by your virtual environment's network configuration.
4. Select **OK** to save the settings to Virtual Machine Properties.

Power on your FortiAuthenticator VM

You can now proceed to power on your FortiAuthenticator VM. Select the name of the FortiAuthenticator VM you deployed in the inventory list and select **Power on the virtual machine** in the **Getting Started** tab. Optionally, you can select the name of the FortiAuthenticator VM you deployed, right-click and select **Power > Power On**.

Initial Configuration

Before you can connect to the FortiAuthenticator VM Web-based Manager you must configure basic network settings via the console tab in your vSphere client. Once configured, you can connect to the FortiAuthenticator VM Web-based Manager and upload the FortiAuthenticator VM license file that you downloaded from the Fortinet Customer Service & Support portal.

The following topics are included in this section:

- FortiAuthenticator VM console access
- Connect to the FortiAuthenticator VM Web-based Manager
- Upload the FortiAuthenticator VM license file
- Configure your FortiAuthenticator VM

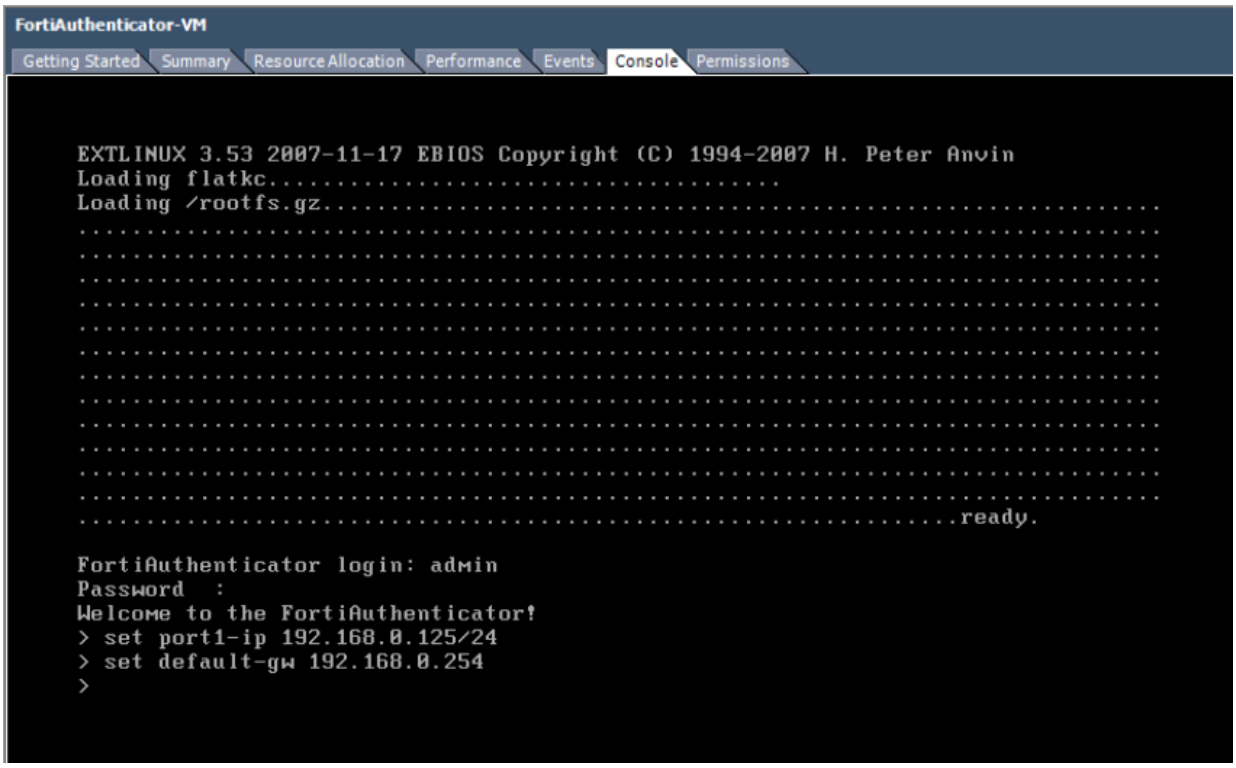
FortiAuthenticator VM console access

To enable Web-based Manager access to the FortiAuthenticator VM you must configure basic network settings of the FortiAuthenticator VM in the vSphere Client Console tab.

To configure basic network settings in FortiAuthenticator VM:

1. In the **Inventory** list, select the FortiAuthenticator VM that you deployed. In the **Getting Started** tab select **Power on the virtual machine**. Optionally, you can right-click the FortiAuthenticator VM and select **Power > Power On**.
2. Select the **Console** tab.
   The **Console** window appears.

   Figure 24: FortiAuthenticator VM console access



3. At the FortiAuthenticator VM login prompt enter the username `admin` and password. The default password is no password.
4. The default `Port1` IP address is set to `192.168.1.99/24`. You can change this IP address with the following CLI command:

   ```
   set port1-ip <address_ipv4/netmask>
   ```

   Where `address_ipv4` is the IPv4 address of the network interface and `netmask` is its network mask. Netmask is expected in the /xx format, for example 192.168.1.1/24.

The Fortinet Customer Service & Support portal currently does not support IPv6 for FortiAuthenticator VM license validation. You must specify an IPv4 address in both the support portal and the port1 management interface.

5. You can configure the static route for the default gateway using the following CLI command:

   ```
   set default-gw <router_ipv4>
   ```

   Where `<router_ipv4>` is the IPv4 address of the gateway router.

Connect to the FortiAuthenticator VM Web-based Manager

Once you have configured the port1 IP address, network mask, and default gateway, launch a web browser and enter the IP address you configured for port1.

To support HTTPS authentication, the FortiAuthenticator VM includes a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiAuthenticator appliance. When you

connect, depending on your web browser and prior access of the FortiAuthenticator VM, your browser might display two security warnings related to this certificate:

The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate. The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

Both warnings are normal for the default certificate. TLS v1.0, TLS v1.1, and TLS v1.2 are supported.

Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.

For details on accepting the certificate, see the documentation for your web browser.

At the login page, enter the user name admin and password and select Login. The default password is no password. The Web-based Manager will appear with an Evaluation License dialog box.

By default, the Web-based Manager is accessible via HTTPS.

Upload the FortiAuthenticator VM license file

Every FortiAuthenticator VM includes a 5-user evaluation license. During this time the FortiAuthenticator VM operates in evaluation mode. Before using the FortiAuthenticator VM you must enter the license file that you downloaded from the Fortinet Customer Service & Support portal upon registration.

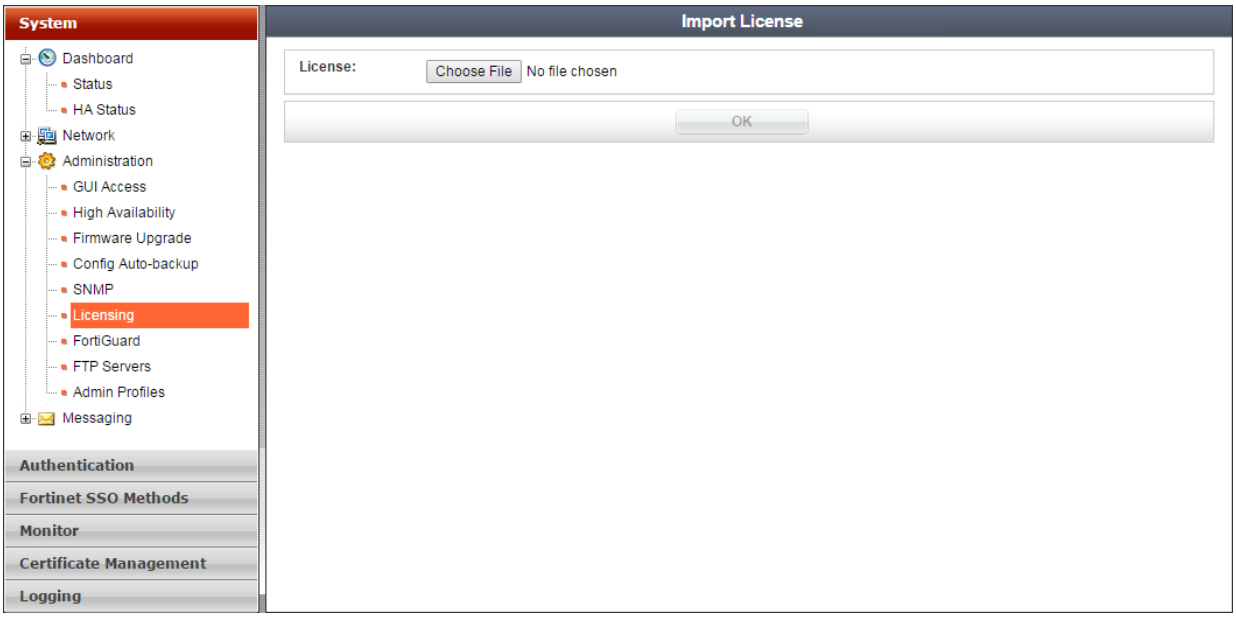
Plan a maintenance window to apply the FortiAuthenticator VM license as the VM will reboot.

As your organization grows, you can simply either allocate more resources or migrate your virtual appliance to a physical server with more power, then upgrade your FortiAuthenticator VM license to support your needs.

To upload the FortiAuthenticator VM license file:

1. Log into the FortiAuthenticator VM.
2. Go to **System > Administration > Licensing**.
   The **Import License** page opens.

   Figure 25: Import License page



3. Select **Choose File** and locate the license file (`.lic`) on your computer. Select **OK** to upload the license file.
4. The VM registration status appears as valid once the license has been validated.

As a part of the license validation process, FortiAuthenticator VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAuthenticator's IP address has been changed, the FortiAuthenticator VM must be rebooted in order for the system to validate the change and operate with a valid license.

5. If the IP address in the license file and the IP address configured in the FortiAuthenticator VM do not match, you will receive the following error message dialog box when you log back into the VM.

Figure 26: VM license file is invalid dialog box

If this occurs, you will need to change the IP address in the Fortinet Customer Service & Support portal to match the management IP and re-download the license file. For information on changing the management IP address, see To edit the FortiAuthenticator VM IP address: on page 1.

After an invalid license file is loaded to FortiAuthenticator VM, the Web-based Manager will be locked until a valid license file is uploaded.

Configure your FortiAuthenticator VM

Once the FortiAuthenticator VM license has been validated you can begin to configure your device. For more information on configuring your FortiAuthenticator VM see the FortiAuthenticator Administration Guide on the Fortinet Document Library.

In VM environments, it is recommended that you use the VMware **Snapshot** utility to backup the VM instance. In the event of an issue with a firmware upgrade or configuration issue, you can use the **Snapshot Manager** to revert the VM instance to a previous **Snapshot**. To create a **Snapshot**, right-click the VM instance and select **Snapshot > Take Snapshot**.